Die Landesbeauftragte für den Datenschutz Niedersachsen

26. Tätigkeitsbericht 2020

Niedersachsen

26. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für das Jahr 2020

Herausgeber: Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5, 30159 Hannover
Postfach 2 21, 30002 Hannover

Verantwortlich: Barbara Thiel

Layout: Bodenstedt Druck-Grafik-Satz GmbH
Ikarusallee 13, 30179 Hannover

Bilder, Grafiken: Seite 9: LfD Niedersachsen
Seite 108, 127: dpa-infografik,
Titelseite, Bildmotiv Grundlayout, alle weiteren: ccPhotoCloud

Druck: Druckerei Albert Funke GmbH
Sorststraße 6, 30165 Hannover

Inhaltsverzeichnis

A. Vorwort

Homeoffice, Online-Vorträge und immer wieder Video-Konferenzen – wie fast überall wurde auch der Alltag meiner Behörde im Jahr 2020 von der Corona-Pandemie bestimmt. Viele Pläne ließen sich aufgrund der veränderten Umstände nicht in die Tat umsetzen. Die Pandemie führte uns zudem eindrücklich vor Augen, wie wichtig eine digitale Infrastruktur für das Funktionieren unserer Gesellschaft mittlerweile ist. Und gleichzeitig nahm die Arbeitslast meiner Behörde erneut deutlich zu.

Manch einer mag bislang gedacht haben, das Thema Datenschutz habe aufgrund des Geltungsbeginns der Datenschutz-Grundverordnung (DS-GVO) lediglich einen kurzfristigen Aufmerksamkeitsschub erhalten und werde alsbald wieder an Bedeutung verlieren. Spätestens seit dem vergangenen Jahr ist klar, dass diese Annahme falsch ist. Ich fragte mich im März 2020 selbst, wie sich Lockdown und Pandemie wohl auf die Fallzahlen meines Hauses auswirken würden. Die Antwort kam schnell: Trotz (und zum Teil auch wegen) Corona schnellten vor allem die Beschwerdezahlen weiter in die Höhe – von mehr als 1800 im Jahr 2019 auf nun fast 2500. Der Anstieg der von Verarbeitern gemeldeten Datenschutzverletzungen von rund 820 auf fast 1000 fiel zwar nicht ganz so drastisch, aber immer noch deutlich aus.

Immer wieder stellt sich angesichts dieser Masse an Einzelfällen die Frage, wie es gelingen kann, dass meine Behörde nicht für andere wichtige Aufgaben gelähmt wird. Denn auch diese werden nicht weniger umfangreich – im Gegenteil:

- Um das Ziel der europäischen Harmonisierung des Datenschutzrechts weiter voranzutreiben, ist vielfältiges und zeitintensives Engagement in den Gremien des Europäischen Datenschutzausschusses notwendig.
- Die Komplexität von Beratungsanfragen nimmt analog zu immer komplexeren Geschäftsmodellen und Verwaltungsprozessen kontinuierlich zu.
- Die wegen Datenschutzverstößen verhängten Bußgelder stoßen in neue (Millionen-)Dimensionen vor, entsprechend aufwändig sind die dafür nötigen Verfahren.

Erschwerend kommt für die Erfüllung meines Auftrags hinzu, dass der Datenschutz noch immer regelmäßig als Begründung dafür herhalten muss, wenn Projekte scheitern oder Mängel publik werden. „Geht nicht wegen Datenschutz", ist ein ebenso grammatikalisch wie faktisch fragwürdiger Satz. In den

Barbara Thiel

meisten Fällen erweist er sich als falsch, wenn man sich die Mühe macht, genauer hinzusehen. Wirtschaftliche und politische Entscheidungsträger sollten nicht der Versuchung erliegen, den Datenschutz vorschnell für Fehlentwicklungen und Probleme verantwortlich zu machen. Das ist ein Reflex, den ich immer wieder beobachten kann, der aber selten den Kern des Problems trifft.

Angemessener Datenschutz ist und bleibt auch in Zukunft eine essenzielle Voraussetzung für den Erfolg der Digitalisierung. Denn nur wenn digitalisierte Datenverarbeitungen transparent und nachvollziehbar gestaltet sind, werden sie auf nachhaltige Akzeptanz in der Bevölkerung stoßen. So lassen sich auch am besten die unbestrittenen Chancen der digitalen Datenverarbeitung nutzen, etwa in der Forschung, in der Früherkennung und Behandlung von Krankheiten oder im Verhältnis zwischen Bürger und Staat. Müssen Menschen dagegen stets fürchten, unterschwellig überwacht, bewertet und gesteuert zu werden, ist es keine Überraschung, wenn zumindest ein Teil von ihnen den Zugriff auf Daten – wo immer möglich – verweigert und die Teilhabe an der digitalen Welt auf ein Minimum beschränkt. Eben das gilt es aber zu verhindern, um die schier unbegrenzten Möglichkeiten der Digitalisierung zum Wohl der Allgemeinheit nutzen zu können.

B. Management Summary

Das Wichtigste in Kürze

Die EU-Kommission bewertet erstmals die Datenschutz-Grundverordnung (DS-GVO), Verantwortliche stehen bei der Übermittlung von Daten in die USA vor neuen Problemen, in Deutschland wird über eine Zentralisierung der Datenschutzaufsicht diskutiert und zum ersten Mal verhängt meine Behörde ein Bußgeld in Millionenhöhe gegen ein niedersächsisches Unternehmen. Auch ohne die Corona-Pandemie wäre das Datenschutzjahr 2020 ereignisreich gewesen.

Evaluation der DS-GVO und erste Streitbeilegung

Kommission stellt Fragmentierung des Rechts fest

Etwas mehr als zwei Jahre nach Geltungsbeginn der DS-GVO legte die Europäische Kommission im Juni 2020 ihren ersten Evaluationsbericht vor. Erwartungsgemäß kam sie darin grundsätzlich zu einem positiven Fazit, gab aber zugleich zu erkennen, dass es für endgültige Schlussfolgerungen noch zu früh sei. Allerdings stellte die Kommission auch fest, dass trotz der Harmonisierung der Datenschutzregelungen noch „eine gewisse Fragmentierung" des Rechts verblieben sei. Auch die vielfach in der Öffentlichkeit wahrgenommene Kritik an der Dauer aufsichtsbehördlicher Kontrollverfahren gegenüber großen Technologiekonzernen in grenzüberschreitenden Fällen griff die Kommission auf, ohne sich aber im Detail mit dieser Frage zu beschäftigen.

Bußgeld gegen Twitter muss erhöht werden

Um einen eben solchen Fall ging es im Herbst im ersten Streitbeilegungsverfahren des Europäischen Datenschutzausschusses (EDSA). Auslöser war ein Beschlussentwurf der federführenden irischen Aufsichtsbehörde gegen Twitter, gegen den mehrere betroffene Aufsichtsbehörden Einspruch eingelegt hatten. Zwar kam der EDSA zu dem Ergebnis, dass die von der irischen Aufsicht verhängte Geldbuße zu niedrig angesetzt war und neu berechnet werden musste. Es zeigte sich bei der Durchführung des Verfahrens aber auch, dass in einigen Fragen noch Klärungsbedarf besteht, zum Beispiel dazu, welchen Inhalt der verbindliche Beschluss des EDSA haben kann. Eine Arbeitsgruppe soll nun Leitlinien zum Streitbeilegungsverfahren erstellen, woran sich auch meine Behörde beteiligt.

Privacy Shield gekippt

Für europaweit großes Aufsehen sorgte am 16. Juli die Entscheidung des Europäischen Gerichtshofs (EuGH) zu „Schrems II". Der Gerichtshof erklärte den Privacy Shield-Beschluss der EU-Kommission für ungültig, auf dessen Grundlage bislang personenbezogene Daten in die USA übermittelt werden konnten. Zwar erachtete der EuGH die Verwendung von Standardvertragsklauseln als weiterhin zulässig, allerdings wurden die Anforderungen an die Datenübermittlung in Länder außerhalb des Europäischen Wirtschaftsraums deutlich erhöht.

Beteiligung an Task Force und Sensibilisierung von Unternehmen

Diese Entscheidung hatte auch wesentlichen Einfluss auf meine Arbeit. Schon im Vorfeld hatte sich meine Behörde maßgeblich an einer Task Force der deutschen Datenschutzaufsichtsbehörden beteiligt, um sich auf das anstehende Urteil und mögliche Entscheidungsszenarien vorzubereiten. Seit November 2020 nehmen Beschäftigte meines Hauses zudem an einer weiteren Task Force teil, die ein gemeinsames Vorgehen der deutschen Aufsichtsbehörden bei der Umsetzung des Urteils gewährleisten soll. Darüber hinaus habe ich im vergangenen Jahr damit begonnen, die niedersächsischen Unternehmen für die Entscheidung des EuGH und die neuen Rahmenbedingungen beim internationalen Datentransfer zu sensibilisieren.

Informationen zum Homeoffice sind gefragt

Obwohl ich erneut sehr stark von meiner Vollzugs- und Aufsichtstätigkeit in Anspruch genommen wurde, war es mir dennoch möglich, auch meinen Aufgaben der Sensibilisierung und Aufklärung nachzukommen. So beteiligte ich mich nicht nur an mehr als 30 Vortrags- und Diskussionsveranstaltungen, sondern veröffentlichte auch wieder zahlreiche Hilfestellungen und Hinweise zu verschiedenen Themen. Besonders gefragt waren im vergangenen Jahr wenig überraschend unter anderem Informationen zum datenschutzgerechten Arbeiten im Homeoffice, zu den Rahmenbedingungen von Videokonferenzen und zum richtigen Umgang mit Daten von Kundinnen und Kunden für die Kontaktverfolgung.

Neue Themen in Zusammenhang mit Corona

Überhaupt sorgte die Corona-Pandemie für einige Mehrarbeit, sei es wegen der (unzulässigen) Übermittlung von Quarantänelisten an die Polizei, der Erhebung von Gesundheitsdaten durch Arbeitgeberinnen und Arbeitgeber oder

die korrekte Ausgestaltung von Attesten zur Befreiung von der Maskenpflicht. Die Pandemie beschleunigte auch die Digitalisierung im Bildungsbereich, legte zugleich aber auch die Schwächen im System offen. Denn Schulen und Hochschulen tragen die Verantwortung für die Auswahl datenschutzkonformer Produkte, um eventuelle Risiken für die Grundrechte der Betroffenen auszuschließen. Sie sind auch in einer Pandemie gefordert, datenschutzkonforme digitale Bildungsangebote zu machen.

Bildungscloud macht Fortschritte

Ein solches Angebot kann die Niedersächsische Bildungscloud (NBC) darstellen, die ich im vergangenen Jahr beratend begleitet habe. Nachdem erste Datenschutzkonzepte deutliche Defizite aufgewiesen hatten, wurden mir im November 2020 überarbeitete Unterlagen vorgelegt, welche die NBC nun deutlich transparenter machten. Es müssen aber weiterhin einige meiner Anforderungen umgesetzt werden. Das betrifft besonders eine nachvollziehbare Darstellung der Datenflüsse und die Sicherstellung der Datenschutzkonformität von Produkten etwaiger Drittanbieter.

Rekord-Bußgeld wegen Videoüberwachung

In völlig neue Dimensionen stieß meine Behörde im vergangenen Jahr im Bußgeldbereich vor. Insgesamt prüfte ich 82 neue Fälle unter Gesichtspunkten einer möglichen Geldbuße und erließ 28 Bußgeldbescheide. Mit 10,4 Millionen Euro war darunter auch das bisher höchste Bußgeld unter Geltung der DS-GVO. Das Unternehmen, gegen das sich der Bescheid richtete, hatte über mindestens zwei Jahre seine Beschäftigten per Video überwacht, ohne dass dafür eine Rechtsgrundlage vorlag.

Viele Bußgeldfälle wegen Videoüberwachung

Überhaupt betrafen auffallend viele Fälle in meiner Bußgeldstelle den Bereich der Videoüberwachung, sei es im Beschäftigtenkontext, im Straßenverkehr oder im privaten Bereich. Besonders zum letztgenannten Bereich erreichten mich 2020 überdurchschnittlich viele Beschwerden. Dabei stieg allerdings auch der Anteil der unbegründeten Beschwerden überproportional. Hier zeigte sich, dass statt einer Beschwerde bei der Aufsichtsbehörde ein offenes Gespräch unter Nachbarn häufig der bessere Weg wäre.

Prüfungen von Unternehmen und Webseiten

Stark begrenzen musste ich im vergangenen Jahr bedauerlicherweise die anlasslosen Kontrollen verantwortlicher Stellen. Zum einen lag dies an den pandemiebedingten Einschränkungen persönlicher Zusammentreffen, zum anderen aber vor allem an mangelnden zeitlichen und personellen Ressourcen. Diesen Hemmnissen zum Trotz konnte ich dennoch Vor-Ort-Kontrollen bei Unternehmen durchführen, die in meiner 2019 abgeschlossenen Querschnittsprüfung deutliche Defizite offenbart hatten. Positiv festzuhalten ist, dass nach diesen Kontrollen auch in bislang defizitär aufgestellten Unternehmen erkannt wurde, dass den Versäumnissen nicht mit Bordmitteln abzuhelfen ist, sondern professionelle Unterstützung notwendig ist.

Wertvolle Erkenntnisse konnte ich zudem durch die Prüfung der Webseiten von 15 niedersächsischen Unternehmen gewinnen. Meine Behörde erlangte auf diesem Weg Informationen darü-

ber, welche datenschutzrechtlichen Standardfehler in diesem Bereich vorherrschen. Diese wurden in einer anschließend veröffentlichten Handreichung mit Hinweisen für die Ausgestaltung von Einwilligungen auf Webseiten aufgegriffen. Die Erfahrungen aus dieser niedersächsischen Prüfung werden sicherlich auch in die Auswertung einer noch laufenden, weiteren Webseiten-Prüfung einfließen, die ich mit den Aufsichtsbehörden mehrerer anderer Bundesländer durchführe.

Prüfung zum Tracking liefert wertvolle Erkenntnisse

Debatte über zentrale Aufsichtsbehörde

Dass die deutschen Aufsichtsbehörden zu solch einem koordinierten, gemeinsamen Vorgehen wie dem gerade beschriebenen in der Lage sind, ist angesichts der Zentralisierungsdebatten des vergangenen Jahres ein wichtiges Signal. Denn auf Antrag des Landes Niedersachsen beriet die Wirtschaftsministerkonferenz im November darüber, ob die Datenschutzaufsicht im Bereich der Wirtschaft in einer Bundesbehörde gebündelt werden sollte.

Letztlich wurde der Antrag erfreulicherweise abgelehnt. Doch die dadurch entstandene Diskussion sollte durchaus dazu genutzt werden, um darüber zu sprechen, ob und inwieweit die rechtlichen Grundlagen für die Zusammenarbeit der Aufsichtsbehörden verbessert werden können. Eine Option hierfür wäre aus meiner Sicht, die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zu institutionalisieren und zum Beispiel rechtsverbindliche Beschlüsse der DSK zu ermöglichen.

Aktivitäten der Datenschutzkonferenz

Unabhängig von ihrer informellen Organisationsform gelang es der DSK auch im vergangenen Jahr, sich deutlich zu verschiedenen datenschutzpolitischen Themen zu positionieren. So kritisierte sie etwa die Pläne des EU-Rats, Polizei und Geheimdiensten den unmittelbaren Zugriff auf verschlüsselte Kommunikationsinhalte von Messenger-Diensten zu gewähren, oder warnte eindringlich vor der Einführung eines verwaltungsübergreifenden Personenkennzeichens, wie es im Zuge der Registermodernisierung vorgesehen ist.

Keine Wirkung zeigten bedauerlicherweise die Bemühungen der DSK in Bezug auf das seit Oktober geltende Patientendaten-Schutz-Gesetz (PDSG). Obwohl die technische Umsetzung der elektronischen Patientenakte noch nicht abgeschlossen ist, verpflichtet das PDSG die gesetzlichen Krankenkassen diese den Versicherten ab 2021 anzubieten. Die Krankenkassen wurden so vom Gesetzgeber in die missliche Situation gezwungen, entweder die Vorgaben des PDSG zu erfüllen oder die Regelungen der DS-GVO einzuhalten. Beides gleichzeitig zu schaffen, ist zumindest 2021 nicht möglich. Aus diesem Grund musste ich auch eine Warnung gegenüber der gesetzlichen Krankenkasse in meinem Zuständigkeitsbereich aussprechen.

Kritik an Personenkennzeichen und Patientendaten-Schutz-Gesetz

C. Europäischer Datenschutz

C.1. Evaluation der DS-GVO

– EU-Kommission zieht positives Fazit

Etwas mehr als zwei Jahre nach Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) hat die Europäische Kommission im Juni 2020 ihren ersten Evaluationsbericht vorgelegt. Erwartungsgemäß kommt die Kommission darin grundsätzlich zu einem positiven Fazit, gibt aber zugleich zu erkennen, dass es für endgültige Schlussfolgerungen noch zu früh sei.

Evaluierungsbericht der Kommission: https://t1p.de/evaluation-dsgvo

Mit etwas Verspätung hat die EU-Kommission am 24. Juni 2020 ihren ersten Evaluierungsbericht nach Art. 97 DS-GVO über die Bewertung und Überprüfung der Grundverordnung dem EU-Parlament und dem Rat vorgelegt. Die Kommission führt darin aus, dass die DS-GVO in den zwei Jahren ihrer Anwendung erfolgreich ihre Ziele erreicht habe, den Schutz des Rechts des Einzelnen auf Schutz seiner personenbezogenen Daten zu stärken und den freien Datenverkehr innerhalb der EU zu gewährleisten.

Allerdings hält es die Kommission für wahrscheinlich, dass die meisten der Themen, die von ihr und von Interessenvertretern für eine Überprüfung im Rahmen der Evaluation identifiziert wurden, von weiteren Erfahrungswerten bei der Anwendung der DS-GVO in den kommenden Jahren profitieren werden. Sie sieht es daher als verfrüht an, bereits jetzt endgültige Schlussfolgerungen hinsichtlich der Anwendung der DS-GVO zu ziehen. Insbesondere sei es noch zu früh, die Funktionsweise der neuen Kooperations- und Kohärenzmechanismen vollständig beurteilen zu können.

Evaluierung der Angemessenheitsentscheidungen verschoben

Zu den Angemessenheitsbeschlüssen[1] hat die Kommission – entgegen dem Auftrag aus Art. 97 DS-GVO – bislang keine Bewertung vorgelegt. Im Bericht verweist die Kommission auf die, aus damaliger Sicht, anstehende EuGH-Entscheidung am 16.07.2020 in Sachen Schrems II [2], welche möglicherweise Klarstellungen liefern werde, die für bestimmte Elemente der Angemessenheitsstandards entscheidend sein könnten. Daher beabsichtigt die Kommission, zu einem späteren Zeitpunkt zur Evaluierung der Angemessenheitsentscheidungen separat zu berichten. Ein entsprechender Bericht wurde bis Reaktionsschluss dieses Berichts noch nicht vorgelegt.

Verbesserungsbedarf bei grenzüberschreitenden Fällen

Zum Kapitel VII über Zusammenarbeit und Kohärenz äußert sich die Kommission nur sehr kompakt: Die Behandlung grenzüberschreitender Fälle müsse EU-weit effizienter und harmonisierter gestaltet werden. Dies gelte insbesondere für einheitliche Zulässigkeitskriterien für Beschwerden und die Dauer der Beschwerdeverfahren aufgrund unterschiedlicher nationaler Fristen oder des Fehlens von Fristen im nationalen Verwaltungsverfahrensrecht.

Mehr Effizienz und Harmonisierung gefordert

1 Ein „Angemessenheitsbeschluss" ist ein Beschluss, der von der Europäischen Kommission gemäß Artikel 45 DS-GVO angenommen wird und durch den festgelegt wird, dass ein Drittland (d. h., ein Land, das nicht an die DS-GVO gebunden ist) oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet.

2 Siehe D.1, S. 27

Die vielfach in der Öffentlichkeit wahrgenommene Kritik an der Dauer aufsichtsbehördlicher Kontrollverfahren gegenüber großen Technologiekonzernen in grenzüberschreitenden Fällen greift die Kommission auf, ohne sich aber im Detail mit dieser Frage zu beschäftigen. Sie betont lediglich die Verpflichtung der Mitgliedstaaten, den nationalen Datenschutzbehörden ausreichende personelle, finanzielle und technische Ressourcen bereitzustellen. In diesem Zusammenhang mutmaßt die Kommission, dass die Datenschutzbehörden in Irland und Luxemburg aufgrund ihrer federführenden Zuständigkeit für die größten multinationalen Technologiekonzerne möglicherweise im Verhältnis zu ihrer Bevölkerung größere Ressourcen benötigten.

Die Entwicklung einer wirklich gemeinsamen europäischen Datenschutzkultur zwischen den Datenschutzbehörden sei noch ein laufender Prozess. Die Behörden hätten die von der DS-GVO bereitgestellten Instrumente, wie z. B. gemeinsame Maßnahmen, die zu gemeinsamen Ermittlungen führen könnten, noch nicht vollständig genutzt.

„Gewisse Fragmentierung" des Rechts

Zu starker Gebrauch von Öffnungsklauseln

Angesichts der Bestrebungen des europäischen Gesetzgebers für eine möglichst kohärente Anwendung des Datenschutzrechts in der Union erscheint die Kritik der Kommission bemerkenswert, dass trotz der Harmonisierung der Datenschutzregelungen noch „eine gewisse Fragmentierung" des Rechts verblieben sei. Grund hierfür sei, dass die Mitgliedstaaten extensiv Öffnungsklauseln der DS-GVO genutzt hätten. Als Beispiel werden die Unterschiede in den Mitgliedstaaten für die Altersgrenze bei der Einwilligung von Kindern in Bezug auf Dienste der Informationsgesellschaft genannt. Die DS-GVO sieht hier eine Altersgrenze von 16 Jahren vor, erlaubt den Mitgliedstaaten aber eine niedrigere Altersgrenze bis zum 13. Lebensjahr. Deutschland hat von dieser Öffnungsklausel keinen Gebrauch gemacht.

Ausblick

Sofern die Kommission in ihrer Evaluierung Regelungsbedarf ermittelt, hat sie gemäß Art. 97 Abs. 5 DS-GVO erforderlichenfalls geeignete Vorschläge zur Änderung der DS-GVO vorzulegen. Im ersten Evaluationsbericht hat die Kommission zwar einige Bereiche identifiziert, in denen zukünftig Verbesserungen möglich sind. Allerdings lässt der Bericht nicht erwarten, dass die Kommission in nächster Zeit einen Vorstoß zu einer Novellierung der DS-GVO unternehmen wird. Das erscheint angesichts der verhältnismäßig kurzen Geltungsdauer der DS-GVO auch folgerichtig.

C.2. Erstes Streitbeilegungsverfahren vor dem Europäischen Datenschutzausschuss

Im Herbst 2020 führte der Europäische Datenschutzausschuss (EDSA) das erste Streitbeilegungsverfahren gemäß Art. 65 Abs. 1 lit. a Datenschutz-Grundverordnung (DS-GVO) durch. Dieses ist für grenzüberschreitende Fälle konzipiert, in denen sich europäische Aufsichtsbehörden nicht einig werden, mit welchem Ergebnis ein Verfahren wegen eines Datenschutzverstoßes abgeschlossen werden soll. Meine Behörde war im Rahmen einer Unterarbeitsgruppe an der Ausarbeitung der Entscheidung des EDSA beteiligt.

Gegenstände des Streitbeilegungsverfahrens waren ein Beschlussentwurf der federführenden irischen Aufsichtsbehörde (DPC) und dagegen erhobene Einsprüche betroffener Aufsichtsbehörden. Auslöser der Ermittlungen der DPC war eine Datenschutzverletzung durch Twitter. Ein Fehler in der Software des Unternehmens hatte zur Folge, dass geschützte Tweets in der mobilen Twitter-Anwendung für Android ohne Wissen der Nutzerinnen und Nutzer ungeschützt für die Öffentlichkeit zugänglich waren. Eine größere Anzahl von Personen im Europäischen Wirtschaftsraum war von dieser Datenpanne betroffen. Der Beschlussentwurf der DPC kam zu dem Ergebnis, Twitter habe gegen die DS-GVO verstoßen, weil die Meldung des Datenschutzverstoßes nicht rechtzeitig erfolgt sei und schlug vor, ein Bußgeld in Höhe von 150.000 bis 300.000 US-Dollar zu verhängen (entspricht 135.000 bis 275.000 Euro).

Datenschutzverletzung bei Twitter

Allerdings wurden die Hintergründe dieser Datenpannenmeldung nicht näher untersucht. Insbesondere nicht, ob die Ursache für die meldepflichtige Datenschutzverletzung selbst einen Verstoß gegen die Anforderungen der DS-GVO darstellt. Ich schloss mich wegen dieser Mängel einem Einspruch gegen den Beschlussentwurf an, der durch den Hamburger Datenschutzbeauftragten (als national federführende Aufsichtsbehörde) eingelegt wurde. Der Einspruch kritisierte ebenfalls, dass keine Verwarnung erteilt worden war und dass die vorgeschlagene Höhe der Geldbuße nicht abschreckend genug sei. Die DPC folgte den Einsprüchen nicht, sondern leitete das Streitbeilegungsverfahren ein.

Die Entscheidung des EDSA

Bei der Durchführung des Streitbeilegungsverfahrens stand der EDSA vor folgender Herausforderung: Die DPC hatte nicht untersucht, ob die Ursache für

die meldepflichtige Datenschutzverletzung selbst einen Verstoß gegen die Anforderungen der DS-GVO darstellt. Gleichzeitig wäre der EDSA nicht in der Lage, eine solche Untersuchung selbst vorzunehmen.

Entscheidung des EDSA: https://t1p.de/edsa-twitter

Der EDSA kam zu dem Ergebnis, dass bezüglich möglicher weiterer Datenschutzverstöße mangels vorliegender Sachverhaltsinformationen keine inhaltliche Entscheidung getroffen werden könne. Stattdessen wurde im vom EDSA verabschiedeten verbindlichen Beschluss ein allgemeiner Hinweis an die Verpflichtung zur besseren Kooperation zwischen der federführenden und den betroffenen Aufsichtsbehörden aufgenommen. Hier hätte ich mir durchaus eine inhaltliche Auseinandersetzung des EDSA mit den von den betroffenen Aufsichtsbehörden aufgeworfenen Fragen erhofft, auch wenn das Nachermittlungen durch die DPC bedeutet hätte. Zwar ist der EDSA keine Aufsichtsbehörde und kann daher selbst keine Sachverhaltsermittlungen durchführen. Aus meiner Sicht könnte er jedoch die federführende Aufsichtsbehörde zu einer neuen Sachverhaltsermittlung verpflichten. Da eine solche Nachermittlung aber in aller Regel nicht innerhalb der starren Monatsfrist bis zum vorgesehenen Erlass des endgültigen Beschlusses durchgeführt werden könnte, müsste hierzu das Streitbeilegungsverfahren beendet und das Verfahren nach Art. 60 DS-GVO neu gestartet werden. Eine entsprechende längere Verfahrensdauer sollte aber in Kauf genommen werden, damit sich der EDSA inhaltlich mit den von den betroffenen Aufsichtsbehörden in den Einsprüchen aufgeworfenen Fragen auseinandersetzen kann.

In Bezug auf die Bußgeldhöhe folgte der EDSA dagegen erfreulicherweise den Argumenten der betroffenen Aufsichtsbehörden und verpflichtete die DPC zu einer Neuberechnung des Bußgeldes, um sicherzustellen, dass das Bußgeld wirksam, verhältnismäßig und abschreckend ist. Die DPC führte daraufhin eine Neuberechnung der Bußgeldhöhe durch und setzte in ihrem endgültigen Beschluss gem. Art. 65 Abs. 6 DS-GVO das Bußgeld auf 500.000 US-Dollar fest (rund 450.000 Euro).

Bei der Durchführung des Streitbeilegungsverfahrens hat sich gezeigt, dass in einigen Fragen noch Klärungsbedarf besteht, beispielsweise hinsichtlich des möglichen Inhaltes des verbindlichen Beschlusses des EDSA. Daher hat das Plenum des EDSA eine Arbeitsgruppe mit der Erstellung von Leitlinien zum Streitbeilegungsverfahren beauftragt, woran sich meine Behörde ebenfalls maßgeblich beteiligt.

C.3. Leitlinien zum maßgeblichen und begründeten Einspruch

Mit der Verabschiedung der Leitlinien 9/2020 zum maßgeblichen und begründeten Einspruch hat der Europäische Datenschutzausschuss (EDSA) wichtige Grundsatzfragen zur Zusammenarbeit der europäischen Aufsichtsbehörden bei grenzüberschreitenden Fällen beantwortet. Hiermit wurde den europäischen Aufsichtsbehörden eine bedeutende Arbeitshilfe an die Hand gegeben.

Im Kooperationsverfahren arbeiten die europäischen Aufsichtsbehörden in grenzüberschreitenden Fällen bei der Entscheidungsfindung zusammen.[1] Grundsätzlich ist das Kooperationsverfahren auf einen Konsens zwischen der federführenden und den betroffenen Aufsichtsbehörden ausgerichtet. Allerdings gibt es immer wieder Fälle, in denen die betroffenen Aufsichtsbehörden nicht mit dem von der federführenden Behörde vorgelegten Beschlussentwurf einverstanden sind. Beispielsweise kann es vorkommen, dass betroffene Behörden nicht darin übereinstimmen, auf welche Weise das Prüfverfahren beendet werden soll (z.B. Bußgeld statt Verwarnung oder zu geringe Bußgeldhöhe). In einem solchen Fall steht es allen betroffenen Aufsichtsbehörden nach Art. 60 Abs. 4 Datenschutz-Grundverordnung (DS-GVO) frei, innerhalb von vier Wochen einen maßgeblichen und begründeten Einspruch gegen einen Beschlussentwurf der federführenden Aufsichtsbehörde einzulegen.

Leitlinien 9/2020 des EDSA (Englisch): https://t1p.de/leitlinien-9-2020

Mit den im Oktober 2020 vorgelegten Leitlinien[2], an denen meine Behörde intensiv über mehrere Wochen mitgearbeitet hat, verfolgt der EDSA das Ziel, ein gemeinsames, europäisches Verständnis der Begriffe „maßgeblich" und „begründet" herzustellen.[3] Art. 4 Nr. 24 DS-GVO enthält zwar eine Legaldefinition des Begriffes „maßgeblicher und begründeter Einspruch", allerdings lässt diese einige relevante Fragestellungen offen, die für die praktische Anwendung der Vorschrift in Streitbeilegungsverfahren gemäß Art. 65 Abs.1 lit. a DS-GVO wichtig sind.

1 Siehe hierzu Tätigkeitsbericht 2019, S. 18.

2 Zunächst wurde am 13. Oktober 2020 eine Fassung zur öffentlichen Konsultation vorgelegt. Im Anschluss wurden die Leitlinien überarbeitet, woran meine Behörde ebenfalls beteiligt war. Anfang März 2021 verabschiedete der EDSA die Leitlinien schließlich.

3 Der EDSA ist hiermit einem Wunsch des europäischen Gesetzgebers nachgekommen, zur Frage des Einspruchs erläuternde Leitlinien herauszugeben, siehe Erw.-Gr. 124 DS-GVO.

Die wichtigsten Aussagen der Leitlinien

Nach den Leitlinien muss der Einspruch, um maßgeblich und begründet zu sein, eine Begründung dafür enthalten, warum eine Änderung des Beschlussentwurfes der federführenden Aufsichtsbehörde vorgeschlagen wird. Außerdem muss aus dem Einspruch die Tragweite der Risiken klar hervorgehen, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der EU ausgehen.

Einfluss auf Bußgeldhöhe möglich

Die Leitlinien stellen klar, dass mit einem relevanten und begründeten Einspruch auch geltend gemacht werden kann, dass über die im Beschlussentwurf berücksichtigten Verstöße hinaus weitere Verstöße gegen die DS-GVO vorliegen. Es soll zudem auch möglich sein, dass der Einspruch Lücken im Beschlussentwurf aufzeigt, welche die Notwendigkeit einer weiteren Untersuchung durch die federführende Aufsichtsbehörde erforderlich machen. Zur Zumessung von Geldbußen wird klargestellt, dass es möglich ist mit dem Einspruch die Elemente anzuzweifeln, die zur Berechnung der Bußgeldhöhe herangezogen wurden. Auf diese Weise können betroffene Aufsichtsbehörden beispielsweise versuchen, über einen Einspruch Einfluss auf die Bußgeldhöhe zu nehmen.

Verfahren nach einem Einspruch

Wird rechtzeitig ein maßgeblicher und begründeter Einspruch eingelegt und schließt sich die federführende Aufsichtsbehörde diesem an, legt sie den betroffenen Aufsichtsbehörden gemäß Art. 60 Abs. 5 Satz 1 DS-GVO einen überarbeiteten Beschlussentwurf zur Stellungnahme vor. Ist die federführende Aufsichtsbehörde dagegen mit dem Einspruch nicht einverstanden oder hält ihn nicht für maßgeblich und begründet, leitet sie das Kohärenzverfahren nach Art. 63 DS-GVO ein, in dem letztlich der EDSA eine verbindliche Entscheidung nach Art. 65 DS-GVO treffen wird.

C.4. E-Privacy-Verordnung rückt erneut in weite Ferne

Die mit der Datenschutz-Grundverordnung (DS-GVO) eingeläutete umfassende europäische Datenschutzreform sollte für den Bereich der elektronischen Kommunikation durch den Erlass der E-Privacy-Verordnung ergänzt werden. Ursprünglich war geplant, dass beide Verordnungen am 25. Mai 2018 in Kraft treten. Ich habe hierzu letztmalig in meinem Tätigkeitsbericht 2017/2018 berichtet. Bedauerlicherweise kann ich nun zwei Jahre später nur wiederholen, dass die Zukunft der E-Privacy-Verordnung nach wie vor ungewiss ist.

Ab dem zweiten Halbjahr 2020 bestand ein kleiner Hoffnungsschimmer, dass die Trilog-Verhandlungen für die E-Privacy-Verordnung beginnen könnten. Denn die Bundesregierung hatte beim Antritt ihrer EU-Ratspräsidentschaft im Juli 2020 versprochen, das Thema der europäischen E-Privacy-Regulierung wiederzubeleben und intensiv voranzutreiben. Zuletzt war Finnland mit diesem Projekt im Februar 2020 während seiner EU-Ratspräsidentschaft gescheitert.

Deutsche Präsidentschaft wollte Verordnung vorantreiben

Die Bundesregierung hielt ihr Versprechen auch ein. Sie nahm den letzten Entwurf der E-Privacy-Verordnung mit dem Überarbeitungsstand des Ausschusses für Telekommunikation von März 2020 als Grundlage und versuchte, Kompromissvorschläge für die strittigen Artikel 6 und 8 zu finden. Es handelt sich hierbei um die Regelungen für die Verarbeitung von Kommunikationsdaten und für die Verwendung von Cookies oder ähnlicher Technologien. Der geplante Art. 8 E-Privacy-VO soll die Nachfolgeregelung der sog. Cookie-Vorschrift in Art. 5 Abs. 3 der E-Privacy-Richtlinie sein.

Vorschlag als zu restriktiv abgelehnt

Auch der Kompromissvorschlag aus Deutschland wurde im November 2020 vom Europäischen Rat als zu restriktiv und zu wirtschaftsfeindlich abgelehnt. Und das obwohl er deutlich mehr Verarbeitungsmöglichkeiten für Kommunikationsinhalte und -metadaten sowie für den Einsatz von Cookies und ähnlichen Technologien vorsah als dies nach aktueller Rechtslage der Fall ist. Damit ist ein zeitnaher Erlass einer E-Privacy-Verordnung wieder in weite Ferne gerückt.

Bereits im Tätigkeitsbericht von 2017/18 habe ich betont, wie wichtig der Erlass einer E-Privacy-Verordnung für Deutschland ist. Die Rechtsunsicherheit in Bezug auf den Datenschutz bei der elektronischen Kommunikation hat sich seit damals noch einmal deutlich erhöht. Erstens hat der Bundesgerichtshof im Planet-49-Verfahren eine Entscheidung getroffen, die von der Position der Konferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder abweicht (siehe F.3, S. 57). Zweitens hat die Corona-Pandemie zu einer enormen Steigerung der elektronischen Kommunikation in allen Lebensbereichen geführt.

Tätigkeitsbericht: 2017/18 https://t1p.de/tb17-18

C.5. Die Cookie-Wall wankt – aktualisierte Leitlinien zur Einwilligung in Webseitennutzung

Der Europäische Datenschutzausschuss (EDSA) hat am 5. Mai 2020 die Leitlinien zur Einwilligung in die Nutzung von Internetseiten aktualisiert. Diese klären insbesondere Fragen zur rechtlichen Beurteilung von Cookie-Walls und zur möglichen Einwilligung durch einfachste Handlungen, wie beispielsweise Weiterscrollen.

Leitlinien des EDSA zur Einwilligung: https://t1p.de/leitlinien-einwilligung

Die Leitlinien 05/2020 zur Einwilligung gemäß der Datenschutz-Grundverordnung (DS-GVO) basieren im Wesentlichen auf den Leitlinien der Artikel-29-Datenschutzgruppe, die bereits am 28. November 2017 angenommen worden waren. In diesem Working Paper (WP) 259 fanden sich detaillierte und allgemeine Ausführungen zu den Anforderungen einer datenschutzkonformen Einwilligung nach den Vorgaben der DS-GVO. Die Leitlinien wurden von der Artikel-29-Datenschutzgruppe noch einmal am 10. April 2018 in einer überarbeiteten Fassung verabschiedet und schließlich vom EDSA gebilligt. Die Änderungen der Leitlinien aus dem Jahr 2020 betrafen im Wesentlichen die genannten Fragestellungen zu Einwilligungen im Internet.

Mit einer Cookie-Wall wird Nutzerinnen und Nutzern bislang der Zugriff auf eine Webseite verweigert, wenn sie nicht mit allen dort eingesetzten Cookies einverstanden sind. In der Praxis werden Cookie-Walls auf zahlreichen Webseiten im Internet eingesetzt, insbesondere auf solchen mit aktuellen und Boulevardnachrichten. Gegenüber dem deutschen Vertreter in der zuständigen Social Media Subgroup habe ich betont, dass eine Cookie-Wall nicht datenschutzkonform ist. Der EDSA hat nun klargestellt, dass diese Praxis unzulässig ist. Nutzerinnen und Nutzern muss der Zugang zu einem Online-Angebot auch dann ermöglicht werden, wenn sie dem Setzen von Cookies nicht zugestimmt haben. Dies gilt zumindest für solche Angebote, die generell kostenfrei sind.

Scrollen ist keine Einwilligung

Zweitens wird klargestellt, dass die einfache Weiternutzung einer Webseite, z. B. durch Scrollen, nicht als wirksame Einwilligung anerkannt wird. Gemäß der Leitlinien des EDSA fehlt hierbei eine eindeutig bestätigende Handlung des Nutzers oder der Nutzerin.

Einwilligungen dürfen nicht erzwungen werden

Der EDSA macht zudem deutlich, dass den Nutzerinnen und Nutzern von Webseiten Tracking nicht aufgedrängt werden darf. Einwilligungen dürfen ebenso wenig erzwungen werden. Die Annahme, dass die Weiternutzung einer Webseite eine Einwilligung bedeutet – wie es sehr häufig in Cookie-Bannern formuliert ist –, widerspricht der von der DS-GVO verlangten Freiwilligkeit. Ich begrüße diese Klarstellungen, da sie zu einer wahrnehmbaren Stärkung des Datenschutzes im Online-Bereich führen. Internetnutzerinnen und -nutzer werden in Bezug auf den Schutz ihrer personenbezogenen Daten davon profitieren.

C.6. Europäische Leitlinien zur Datenverarbeitung bei vernetzten Fahrzeugen

Ein Schlüsselthema in der Automobilindustrie und gleichzeitig ein wichtiges Tätigkeitsfeld für den Datenschutz ist die vernetzte Mobilität. Fahrzeuge werden immer umfassender mit Informations- und Kommunikationssystemen ausgestattet, um eine Vernetzung zwischen Verkehrsteilnehmenden und Infrastruktur zu ermöglichen. Staus und langwierige Parkplatzsuchen können so vermieden, Verkehrsverstöße verhindert und negative Umwelteinflüsse reduziert werden. Das erfordert eine Unmenge von – in der Regel – personenbezogenen Datenverarbeitungen.

Leitlinien zu vernetzten Fahrzeugen (Englisch): https://t1p.de/leitlinien-vernetzt

Wegen der Datenfülle in Zusammenhang mit der vernetzten Mobilität ist es sehr zu begrüßen, dass der Europäische Datenschutzausschuss (EDSA) mit den Leitlinien 1/2020 zur Verarbeitung personenbezogener Daten im Kontext von vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen Stellung genommen hat. Die Leitlinien befassen sich mit den datenschutzrechtlichen Anforderungen bei der Erfassung der Daten im Fahrzeug sowie deren Übertragung an Geräte des Benutzers oder der Benutzerin selbst und an weitere externe Empfängerinnen und Empfänger.

Im ersten Teil der Leitlinien werden vor allem der Anwendungsbereich und die wichtigsten Definitionen erläutert. Teil zwei befasst sich mit den generellen datenschutzrechtlichen Anforderungen und enthält allgemeine Empfehlungen zum Datenschutz. Der dritte Teil erläutert praxisorientiert anhand von fünf Fällen mögliche Rechtsgrundlagen, Beteiligte der Datenverarbeitungen, den Umgang mit Betroffenenrechten und Ansätze für die Gewährleistung der Sicherheit der Verarbeitung. Inhaltlich hat der EDSA einige grundlegende Entscheidungen getroffen, durch die Auslegungsfragen der Wissenschaft und Praxis beantwortet werden.

Anwendungsbereich

Die Leitlinien betreffen die Verarbeitung personenbezogener Daten im Zusammenhang mit der nicht-beruflichen Nutzung von vernetzten Fahrzeugen durch betroffene Personen: z. B. Fahrer (-innen), Mitfahrer (-innen), Fahrzeugbesitzer (-innen), Mieter (-innen). Als mobilitätsbezogene Anwendungen werden insbesondere solche des Mobilitäts- und Fahrzeugmanagements, der Verkehrssicherheit, der Fahrerassistenz sowie des Entertainments aufgeführt.

Ausdrücklich aus dem Anwendungsbereich der Leitlinien ausgeklammert werden:

- Firmenfahrzeuge und damit der Beschäftigtendatenschutz,
- die Möglichkeit der passiven Verfolgung durch WiFi- oder Bluetooth-Tracking,
- integrierte Bildaufzeichnungsgeräte, wie z. B. Parkkameras oder Dashcams und
- eingebundene kooperative intelligente Verkehrssysteme (C-ITS).[1]

Firmenwagen und Dashcams ausgeklammert

Fahrzeugdaten sind in der Regel personenbezogen

Eine aus Sicht der Datenschützer erfreulich deutliche Position hat der EDSA zu der bislang in Wissenschaft und Praxis uneinheitlich beantworteten Frage des Personenbezugs von Fahrzeugdaten eingenommen. Bereits in der Einleitung wird ausgeführt, dass die meisten der zahlreichen durch vernetzte Fahrzeuge erzeugten Daten als personenbezogen zu betrachten sind, da sie sich unmittelbar oder zumindest mittelbar auf Fahrer, Fahrerin oder Passagiere beziehen.

Besonders schützenswerte Datenkategorien

In den Leitlinien werden drei Datenkategorien, die von vernetzten Fahrzeugen erzeugt werden, besonders hervorgehoben, da es sich um besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs 2 DS-GVO handelt oder ihre Verarbeitung mit besonderen Risiken für die Rechte und Interessen der betroffenen Personen einhergehen.

Im Einzelnen handelt es sich um

- Standortdaten,[2]
- biometrische Daten gemäß Art. 4 Nr. 14 DS-GVO[3] und
- personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten[4], s. Art. 10 DS-GVO.

Allgemeine Empfehlungen

Darüber hinaus orientieren sich die allgemeinen Empfehlungen an den Grundsätzen der Verarbeitung gemäß Art. 5 DS-GVO sowie an den daraus abgeleiteten konkreten datenschutzrechtlichen Pflichten der Verantwortlichen. Einen besonderen Fokus legen die Leitlinien bei den Empfehlungen zum einen darauf, dass insbesondere aufgrund der Vielzahl der (möglichen) Verantwortlichen der Datenverarbeitung den Betroffenen die Wahrnehmung ihrer Betroffenenrechte weitmöglichst zu

1 Siehe hierzu die Stellungnahme der Art. 29 Arbeitsgruppe Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-IST). Abrufbar unter https://t1p.de/CIST.

2 Offen bleibt, ob die geolocation data" mit den in Art. 2 lit. c 2092/58/EG legaldefinierten „location data" gleichzusetzen sind. Die Vorschrift definiert Standortdaten als diejenigen „Daten, die in einem elektronischen Kommunikationsnetz oder von einem elektronischen Kommunikationsdienst verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben".

3 Biometrische Daten werden für die Authentifizierung des Halters oder von Fahrern verwendet, beispielsweise um das Fahrzeug per Fingerabdruck öffnen und schließen zu können oder Profileinstellungen und Präferenzen eines Fahrers automatisch zu erkennen und anzupassen.

4 In den Guidelines wird als Beispiel für deliktsbezogene Daten die momentane Geschwindigkeit eines Fahrzeugs in Kombination mit genauen Geolokalisierungsdaten oder Daten, die darauf hinweisen, dass das Fahrzeug eine weiße Linie überquert hat, angeführt.

Besondere Bedeutung von Privacy by Design

erleichtern ist. Zum anderen wird die besondere Bedeutung der datenschutzrechtlichen Ansätze Privacy by Design und Privacy by Default hervorgehoben. Hierzu werden auch allgemeine Ansätze wie die lokale Datenverarbeitung im Fahrzeug sowie frühestmögliche Anonymisierung und Pseudonymisierung dargestellt. Schließlich finden sich umfassende Ausführungen zur Erfüllung der datenschutzrechtlichen Informationspflichten gegenüber Betroffenen.

Dem EDSA ist es selbstverständlich nicht möglich, ein so umfassendes, komplexes und zudem noch in der Entwicklung befindliches Thema abschließend in den Leitlinien datenschutzrechtlich zu bewerten. Umso begrüßenswerter ist es aber, dass der Ausschuss dennoch die Gelegenheit ergriffen hat, zukunftsgerichtet wesentliche datenschutzrechtliche Leitplanken für vernetzte Fahrzeuge und mobilitätsbezogene Anwendungen zu formulieren. Es ist zu hoffen, dass der in diesem Bereich so wichtige Ansatz der datenschutzfreundlichen Technikentwicklung dadurch erheblich gefördert und in der Praxis umgesetzt wird.

D. Internationaler Datenverkehr

D.1. EuGH annulliert Privacy Shield und stellt erhöhte Anforderungen an Datentransfers in Drittstaaten

Mit seinem Grundsatzurteil zu „Schrems II“ vom 16. Juli 2020 hat der Europäische Gerichtshof (EuGH) den Privacy Shield-Beschluss der EU-Kommission für ungültig erklärt, auf dessen Grundlage bislang personenbezogene Daten in die USA übermittelt werden konnten. Zwar hat der EuGH die Verwendung von Standardvertragsklauseln als weiterhin zulässig erachtet, allerdings wurden die Anforderungen an die Datenübermittlung in Länder außerhalb des Europäischen Wirtschaftsraums deutlich erhöht. Verantwortliche sind daher in der Pflicht, ihre Datenexporte in die USA und andere Drittländer zu überprüfen und gegebenenfalls auf neue rechtliche Grundlagen zu stützen sowie eventuell zusätzliche Schutzmaßnahmen zu ergreifen.

Der grenzüberschreitende Datenverkehr ist aus dem Alltag vieler niedersächsischer Unternehmen nicht mehr wegzudenken. Die Globalisierung des Welthandels und die weltweite elektronische Vernetzung haben dazu beigetragen, dass der internationale Datenverkehr und insbesondere die Übermittlung personenbezogener Daten an Länder außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung (sog. „Drittländer“) enorm an Bedeutung gewonnen haben. Durch diese internationalen Kommunikations- und Handelsbeziehungen sind allerdings auch neue Herausforderungen für den Schutz personenbezogener Daten entstanden. Die Datenschutz-Grundverordnung (DS-GVO) will diese Datenströme nicht unterbinden. Sie verfolgt aber das Ziel, dass das durch die DS-GVO unionsweit gewährleistete Schutzniveau für natürliche Personen bei der Übermittlung an Empfängerinnen und Empfänger in Drittländer nicht untergraben wird. Daher ist es von grundlegender Bedeutung für den Schutz personenbezogener Daten, dass die Anforderungen der DS-GVO für die Datenübermittlung in Drittländer eingehalten werden.

Schon frühe Zweifel am Privacy Shield

Auf der Grundlage der Privacy Shield-Übereinkunft zwischen der EU und den USA hatte die EU-Kommission 2016 in einem Durchführungsbeschluss festgestellt, dass die USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleisten. Das hatte zur Folge, dass personenbezogene Daten beim Vorliegen einer allgemeinen Rechtsgrundlage auf der Grundlage des Art. 45 DS-GVO in die USA übermittelt werden durften, wenn die empfangenden Stellen unter dem Privacy Shield zertifiziert waren.

Schon seit dem Inkrafttreten des Privacy Shield waren allerdings immer wieder Zweifel an dessen Wirksamkeit laut geworden. Zuletzt hatte der Europäische Datenschutzausschuss (EDSA) 2019 deutliche Kritik geäußert und insbesondere den fehlenden gerichtlichen Rechtsschutz europäischer Betroffener gegenüber Datenzugriffen von US-Behörden bemängelt.

Überprüfungsbericht des EDSA zu Privacy Shield 2019 (Englisch): https://t1p.de/edsa-shield

Des Weiteren wurde die Funktion der vom Privacy Shield vorgesehenen Ombudsperson kritisiert, deren Aufgabe es war, Beschwerden von Bürgerinnen und Bürgern aus der Europäischen Union in Bezug auf den Datenzugriff durch nationale Sicherheitsbehörden zu überprüfen. Allerdings verblieben Zweifel an der Unabhängigkeit der Ombudsperson und daran, ob diese mit hinreichenden Befugnissen ausgestattet war, um an Informationen zu gelangen und Datenschutzverstöße der Nachrichtendienste abzustellen.

EuGH kippt Privacy Shield

Ausgangspunkt des Rechtsstreits vor dem EuGH war eine Beschwerde Maximilian Schrems'. Schrems hatte bei der irischen Datenschutzaufsichtsbehörde eine Beschwerde eingelegt, dass Facebook Irland seine personenbezogenen Daten an die Facebook, Inc. in den USA übermittelt. Facebook setzte diesbezüglich Standardvertragsklauseln ein (Art. 46 Abs. 2 Buchstabe c DS-GVO). In erster Linie hatte der EuGH daher nur über die Datenübermittlung auf der Grundlage von Standardvertragsklauseln zu befinden, nicht über den Privacy Shield. Der EuGH sah eine Entscheidung über den Privacy Shield allerdings als erforderlich an. Denn solange der Privacy Shield Bestand hatte, hätte eine auf Standardvertragsklauseln gestützte Übermittlung personenbezogener Daten an ein Unternehmen, das (wie Facebook, Inc.) in der Privacy-Shield-Liste aufgeführt war, im Einzelfall nicht untersagt werden können.

EuGH-Urteil zu Schrems II: https://t1p.de/eugh-schrems

Mit seiner Grundsatzentscheidung „Schrems II" vom 16. Juli 2020 erklärte der EuGH den Beschluss 2016/1250 der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA (Privacy Shield) für unwirksam. Die Luxemburger Richter teilten die Zweifel des EDSA und begründeten ihre Entscheidung damit, dass die US-Überwachungsprogramme nicht auf das zwingend erforderliche Maß begrenzt seien. Mit Blick auf die (Un-)Verhältnismäßigkeit der Zugriffe durch US-Behörden auf personenbezogene Daten von Europäerinnen und Europäern bestehe daher keine Gleichwertigkeit zum Unionsrecht. Ferner teilte der EuGH die Kritik am vorgesehenen Ombudsmechanismus und daran, dass es keinen gleichwertigen gerichtlichen Rechtsschutz für europäische Betroffene gab. Die Übermittlung personenbezogener Daten in die USA auf der Grundlage des Privacy Shield war daher seit dem 16. Juli 2020 unzulässig und musste unverzüglich eingestellt werden. Eine Übergangsfrist, in der personenbezogene Daten noch auf der Grundlage des Privacy Shield in die USA hätten übermittelt werden dürfen, gewährte der EuGH ausdrücklich nicht.

Standardvertragsklauseln bleiben gültig

Die Entscheidung 2010/87/EG der Europäischen Kommission über Standardvertragsklauseln ist nach dem Urteil grundsätzlich weiterhin gültig geblieben, allerdings hat der EuGH die Anforderungen deutlich erhöht. Bei Standardvertragsklauseln handelt es sich um von der EU-Kommission herausgegebene Vertragsmuster, auf deren Grundlage Datenexporteure und -importeure Vereinbarungen über den Datenschutz schließen können, um europäische Datenschutzstandards auch im Drittland zu gewährleisten. Datenübermittlungen in Drittländer dürfen künftig allerdings nur dann auf die Verwendung von Standardvertragsklauseln gestützt werden, wenn die Rechte der betroffenen Personen im Drittland ein gleichwertiges Schutzniveau wie in der Europäischen Union genießen.

Verantwortliche Datenexporteure müssen folglich vor dem Einsatz von Standardvertragsklauseln die Rechtsordnung des Drittlandes sorgfältig bewerten und dabei insbesondere die in Art. 45 Abs. 2 der DS-GVO genannten Kriterien untersuchen, beispielsweise das Vorhandensein wirksamer verwaltungsrechtlicher und gerichtlicher Rechtsbehelfe für Betroffene. Soweit das Recht eines Drittlands bezogen auf den Zugriff nationaler Sicherheits- oder Strafverfolgungsbehörden auf personenbezogene Daten zu Überwachungszwecken in den Blick genommen wird, können die Empfehlungen 02/2020 des EDSA zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen vom 10. November 2020 eine Hilfestellung bei der Beurteilung geben, ob ein gerechtfertigter Eingriff vorliegt.

Empfehlungen des EDSA 02/2020: https://t1p.de/empfehlungen-2-2020

Zusätzliche Maßnahmen können erforderlich sein

Für den Fall, dass Verantwortliche zu dem Ergebnis gelangen, dass im Drittland kein gleichwertiges Schutzniveau vorhanden ist, hat der EuGH die Möglichkeit eröffnet, zusätzliche Maßnahmen zur Sicherstellung eines dem in der Europäischen Union gleichwertigen Schutzniveaus zu ergreifen. Denkbar sind rechtliche, technische oder organisatorische Maßnahmen. Der EDSA hat hierzu als Orientierungshilfe die Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten verabschiedet. Die Empfehlungen beinhalten im Anhang Positiv- und Negativbeispiele für zusätzliche Maßnahmen. Beispielsweise kommt als technische Maßnahme der Einsatz einer starken Verschlüsselung in Betracht, sofern durch diese sichergestellt werden kann, dass die Daten im Drittland zu keinem Zeitpunkt im Klartext vorliegen. Für Anforderungen an eine Verschlüsselung kann auf die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zurückgegriffen werden.

Empfehlungen des EDSA 01/2020: https://t1p.de/empfehlungen-1-2020

Empfehlungen des BSI: https://t1p.de/bsi-01 und https://t1p.de/bsi-02

Falls Verantwortliche zu dem Schluss gelangen, dass unter Berücksichtigung der Umstände der auf Standardvertragsklauseln gestützten Übermittlung und etwaiger zusätzlicher Maßnahmen keine angemessenen Garantien gewährleistet sind, besteht die Verpflichtung, die Übermittlung personenbezogener Daten auszusetzen oder zu beenden. Beabsichtigen Verantwortliche dagegen, die Daten trotz dieser Schlussfolgerung weiterhin in unsichere Drittländer zu exportieren, ist dies der zuständigen Datenschutzaufsichtsbehörde anzuzeigen. Bei mir sind solche Anzeigen bisher nicht eingegangen. Sofern die Aufsichtsbehörde zu der Überzeugung gelangt, dass die Standardvertragsklauseln im Drittland nicht eingehalten werden oder eingehalten werden können und dass der nach dem Unionsrecht erforderliche Schutz der übermittelten Daten nicht mit anderen Mitteln gewährleistet werden kann, kann sie die Aussetzung einer solche Übermittlung anordnen oder diese verbieten.

Datenexporte ausnahmsweise auf der Grundlage von Art. 49 DS-GVO

Falls für ein Drittland weder ein Angemessenheitsbeschluss der EU-Kommission vorliegt[1] noch eine geeignete Garantie im Sinne von Art. 46 DS-GVO (z. B. Standardvertragsklauseln) in Betracht kommt, kann in Erwägung gezogen werden, die Ausnahmevorschrift des Art. 49 DS-GVO zu nutzen, sofern deren Tatbestandsvoraussetzungen erfüllt sind. Aufgrund des Vorhandenseins dieser Vorschrift sah es der EuGH nicht als erforderlich an, eine Übergangsfrist für den Privacy Shield zu gewähren. Grundsätzlich ist die Ausnahmevorschrift des Art. 49 DS-GVO allerdings restriktiv anzuwenden, weil die personenbezogenen Daten auf dieser Grundlage ohne jegliche datenschutzrechtlichen Schutzvorkehrungen übermittelt werden. Einige Ausnahmetatbestände für Datenübermittlungen dürfen auch nur gelegentlich angewendet werden (Erwägungsgrund 111 DS-GVO). Auch bei den übrigen Ausnahmetatbeständen, die keine Beschränkung auf gelegentliche Übermittlungen enthalten, darf nicht gegen das Wesen des Art. 49 DS-GVO als Ausnahmeregelung verstoßen werden. Die diesbezüglich 2018 verabschiedeten Leitlinien des EDSA sind weiterhin gültig und unverändert anzuwenden.

EDSA-Leitlinien 2/2018: https://t1p.de/leitlinien-art49

Sensibilisierung und Beratung durch die Aufsichtsbehörden

Ungeachtet der primären Verantwortung der niedersächsischen Unternehmen und Behörden ist mir bewusst, dass den Datenschutzaufsichtsbehörden eine Schlüsselrolle bei der Information und Beratung zukommt, wie das Urteil des EuGH rechtskonform umgesetzt werden kann. Demgemäß hat sich die Datenschutzkonferenz schon früh zu den Auswirkungen des Urteils positioniert.[2] Außerdem hat der EDSA eine ausführliche Zusammenstellung von Antworten auf häufig zum Urteil gestellte Fragen erarbeitet.[3] Weiter hat der EDSA einen aus sechs Schritten bestehenden Ablaufplan vorgelegt, der Verantwortlichen eine Hilfestellung gibt, welche konkreten Prüfschritte bei der Übermittlung personenbezogener Daten in Drittstaaten durchlaufen werden sollten. Dieser ist in den oben genannten Empfehlungen 01/2020 enthalten.

Die „Schrems II"-Entscheidung hatte 2020 auch wesentlichen Einfluss auf die Arbeit meiner Behörde. Schon im Vorfeld hatte sich meine Behörde maßgeblich an einer Task Force der deutschen Datenschutzaufsichtsbehörden beteiligt, um sich auf das anstehende Urteil und mögliche Entscheidungsszenarien vorzubereiten. Seit November 2020 nimmt meine Behörde zudem an einer weiteren von der DSK eingesetzten Task Force teil, die ein gemeinsames Vorgehen der deutschen Aufsichtsbehörden bei der Umsetzung des Urteils gewährleisten soll. Darüber hinaus habe ich im vergangenen Jahr damit begonnen, die niedersächsischen Unternehmen für das Urteil und die neuen Rahmenbedingungen beim internationalen Datentransfer zu sensibilisieren und werde dies auch in diesem Jahr fortsetzen und intensivieren.

1 Angemessenheitsbeschlüsse der EU-Kommission bestehen für Andorra, Argentinien, Guernsey, die Färöer-Inseln, die Isle of Man, Israel, Japan, Jersey, Kanada, Neuseeland, die Schweiz und Uruguay.

2 Abrufbar unter: https://t1p.de/dsk-schrems2

3 Abrufbar unter: https://t1p.de/faq-schrems2

D.2. Binding Corporate Rules der Novelis-Gruppe bestätigt

Vor ihrer eigentlichen Genehmigung müssen Binding Corporate Rules (BCR) das in der Datenschutz-Grundverordnung (DS-GVO) festgeschriebene Kohärenzverfahren durchlaufen. Im vergangenen Jahr hat der Europäische Datenschutzausschuss (EDSA) erstmals BCR anerkannt, die unter der Federführung meiner Behörde erstellt worden waren.

Liegt kein Angemessenheitsbeschluss vor, dürfen Verantwortliche oder Auftragsverarbeiter personenbezogene Daten an Drittländer oder internationale Organisationen nur übermitteln, sofern diese hierfür geeignete Garantien vorgesehen haben (Art. 46 Abs. 1 DS-GVO). Diese Garantien sollen ein angemessenes Datenschutzniveau gewährleisten, das mit dem in der EU vergleichbar ist. Als Möglichkeit zur Erbringung „geeigneter Garantien" sieht Art. 46 Abs. 2 lit. b) in Verbindung mit Art. 47 DS-GVO „verbindliche interne Datenschutzvorschriften" vor. In der Praxis hat sich die Verwendung des englischen Begriffs „Binding Corporate Rules" etabliert.

BCR können insbesondere bei international tätigen Konzernen mit internem Datenfluss in Drittländer empfehlenswert sein. Dabei legt das Unternehmen Regelungen für den Umgang mit personenbezogenen Daten auch in Drittländern fest, in denen Konzerngesellschaften grundsätzlich nicht an die DS-GVO gebunden wären. Die BCR müssen daher einen Schutz bieten, der im Wesentlichen der DS-GVO entspricht.

Schutzniveau durch BCR muss dem der DS-GVO entsprechen

Die BCR stehen unter einem Genehmigungsvorbehalt der zuständigen Aufsichtsbehörde, die zunächst das Kohärenzverfahren nach Art. 63, 64 Abs. 1 DS-GVO einleitet. Ein solches Verfahren setzt voraus, dass eine grenzüberschreitende Verarbeitung im Sinne von Art. 4 Nr. 23 DS-GVO vorliegt. Das heißt, dass auf der Grundlage der BCR Datenübermittlungen aus mehr als einem Mitgliedstaat vorgesehen sind oder erhebliche Auswirkungen auf Betroffene in anderen Mitgliedstaaten haben können.

Erstes Verfahren nach DS-GVO unter niedersächsischer Federführung

Bereits im Jahr 2018 stellte die Novelis-Gruppe – ein Unternehmen mit Hauptsitz in Niedersachsen und weltweiten Niederlassungen – bei meiner Behörde einen Antrag auf Genehmigung der eigenen BCR. Im Jahr 2020 habe ich in diesem Zusammenhang erstmals als federführende Aufsichtsbehörde ein Kohärenzverfahren zur Genehmigung von BCR eingeleitet.

Dem Kohärenzverfahren vorgeschaltet war das sogenannte Kooperationsverfahren. Die Aufgabe meiner Behörde bestand darin, als alleinige Ansprechpartnerin für das Unternehmen zu fungieren und den Prozess bis zur Genehmigung der BCR zu begleiten. Unter Beteiligung der italienischen Aufsichtsbehörde als Co-Prüferin begutachtete ich umfassend die BCR auf ihre Vereinbarkeit mit den Vorgaben der DS-GVO, unter anderem die Einhaltung der Betroffenenrechte und die Implementierung angemessener technisch-organisatorischer Maßnahmen. In mehreren Beratungsgesprächen diskutierte ich die Anmerkungen und Änderungswünsche mit dem Unternehmen, das die Regelungen der BCR entsprechend anpasste. Anschließend wurde allen im EDSA vertretenen Aufsichtsbehörden die Gelegenheit gegeben, den konsolidierten Entwurf der BCR zu prüfen.

Nachdem dieses Verfahren erfolgreich abgeschlossen war, habe ich das eigentliche Kohärenzverfahren nach der DS-GVO förmlich eingeleitet und eine Stellungnahme des EDSA nach Art. 64 Abs. 1 lit. f DS-GVO beantragt. Der EDSA hat seine Stellungnahme zu den BCR der Novelis-Gruppe im Dezember 2020 angenommen.

Stellungnahme des EDSA: https://t1p.de/bcr-novelis

Die abschließende Genehmigung der BCR durch meine Behörde wurde zu Beginn des Jahres 2021 erteilt. Diese ist für alle Aufsichtsbehörden in der Europäischen Union und im Europäischen Wirtschaftsraum bindend.

E. Datenschutzkonferenz

E.1. Zentralisierung der Datenschutzaufsicht – niedersächsischer Vorschlag scheitert

Im vergangenen Jahr hat das Niedersächsische Wirtschaftsministerium mit der Anmeldung des Themas „Vereinheitlichung der Datenschutzaufsicht für den Markt" zur Wirtschaftsministerkonferenz (WMK) eine bundesweite Debatte über eine Neuorganisation der Datenschutzaufsicht im nichtöffentlichen Bereich angestoßen. Die WMK hat sich gegen den Antrag Niedersachsens ausgesprochen, zugleich aber die Notwendigkeit einer einheitlichen und verbindlichen Auslegung von datenschutzrechtlichen Anforderungen betont. Auch ich sehe in dieser Beziehung Verbesserungspotenzial bei der Zusammenarbeit der Aufsichtsbehörden. Die Diskussion um eine grundlegende Neuorganisation der Aufsicht halte ich indes für deutlich verfrüht.

Auf Antrag des Landes Niedersachsen, der bereits im April 2020 eingebracht worden war, berieten die Wirtschaftsminister im November 2020 über eine Zentralisierung der Datenschutzaufsicht im Bereich der Wirtschaft. Begründet wurde der Antrag mit der auch von der Datenethikkommission der Bundesregierung vertretenen Auffassung, dass „in der in Einzelfragen abweichenden Auslegung von datenschutzrechtlichen Anforderungen und der divergierenden Vollzugspraxis eine zusätzliche Belastung deutscher Unternehmen im (…) Bereich der Datenschutz-Compliance" gesehen werde.

Schlussendlich sprach sich die Wirtschaftsministerkonferenz gegen konkrete Zentralisierungsvorschläge aus, sah aber auch die Notwendigkeit einer einheitlichen und verbindlichen Auslegung von datenschutzrechtlichen Anforderungen. Sie bat daher die Bundesregierung, gemeinsam mit den Ländern und den Datenschutzaufsichtsbehörden die bestehenden Regelungen in §§ 17 ff. Bundesdatenschutzgesetz (BDSG) auf praktische Durchführbarkeit und Verbesserungspotenzial bei der Zusammenarbeit zu überprüfen.

Beschlüsse der WMK vom 30.11.20: https://t1p.de/wmk-beschluss

Empfehlungen der Datenethikkommission

Gutachten der Datenethikkommission: https://t1p.de/dek-gutachten

Ausgangspunkt für den Beschlussvorschlag des Niedersächsischen Wirtschaftsministeriums waren die Empfehlungen der Datenethikkommission. In ihrem Gutachten vom Oktober 2019 attestierte die Kommission den deutschen Datenschutzaufsichtsbehörden von Bund und Ländern Abweichungen in Aussagen zu datenschutzrechtlichen Anforderungen und eine divergierende Vollzugspraxis. Das föderale Miteinander der Datenschutzbehörden der Bundesländer habe bisher keine ähnliche Verbindlichkeit und Einheitlichkeit erreicht wie dies mit dem Europäischen Datenschutzausschuss auf europäischer Ebene geschehen sei. Für den Fall, dass sich eine einheitliche und kohärente Anwendung der DS-GVO nicht durch eine verbesserte und formalisierte Abstimmung unter den deutschen Aufsichtsbehörden gewährleisten lasse, schlug die Datenethikkommission vor, die Datenschutzaufsicht im nichtöffentlichen Bereich bei einer Stelle zu konzentrieren, beispielsweise beim Bundesbeauftragen für den Datenschutz und die Informationssicherheit oder durch Gründung einer gemeinsamen Einrichtung der Länder.

Zentralisierungsdebatte ist deutlich verfrüht

Es dürfte unstreitig sein, dass die Aufsichtsbehörden von Bund und Ländern nicht immer zu einheitlichen Auffassungen gelangen. Diese Tatsache ist für sich genommen zunächst einmal kein Grund, das föderale System in Deutschland im Bereich des Datenschutzes grundsätzlich in Frage zu stellen. Dort, wo um die Auslegung von Rechtsfragen gerungen wird, ist es nicht ungewöhnlich, dass die Meinungen auseinander gehen. Gerade die Pluralität der Rechtsmeinungen erzeugt vertiefte Diskussion sowie differenzierte Betrachtung und kann auch als besonderer Vorteil gewertet werden, verfügt doch gerade Deutschland im Datenschutzrecht über eine lange Tradition und daraus resultierend über eine hohe Expertise. Außerdem darf nicht verkannt werden, dass die Herausbildung einer einheitlichen Rechts- und damit auch einer einheitlichen Anwendungspraxis bei neuen Gesetzen – zumal von einer Tragweite wie bei der DS-GVO – hinreichend Zeit benötigt.

Infothek unter: https://www.datenschutzkonferenz-online.de

Im Übrigen hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) seit Geltung der DS-GVO eine Vielzahl von Auslegungshilfen zum neuen Recht bereitgestellt, um zur Rechtssicherheit beizutragen, beispielsweise Kurzpapiere, Orientierungshilfen und andere rechtliche Positionsbestimmungen. Zudem ist mittlerweile in der Geschäftsordnung der DSK geregelt, dass die rechtlichen Fragestellungen mit einfacher Mehrheit und nicht einvernehmlich zu entscheiden sind. Diese positive Entwicklung sollte aus meiner Sicht wohlwollend wahrgenommen, begleitet und ausgebaut werden. Denn auch die Datenethikkommission fordert eine Vereinheitlichung der Datenschutzaufsicht über die Wirtschaft durch eine neue Behördenstruktur erst dann, wenn die notwendige Abstimmung tatsächlich nicht gelingt. Dies bleibt abzuwarten und sollte nicht voreilig organisatorischen Überlegungen geopfert werden. Gleichwohl sehe auch ich an dieser Stelle noch Optimierungspotenziale insbesondere in verfahrensrechtlicher Hinsicht.

Das Bundesinnenministerium führt zurzeit eine Evaluierung des BDSG durch. Dabei wird es auch – u.a. im Dialog mit den Aufsichtsbehörden – um die Frage gehen, ob und inwieweit die rechtlichen Grundlagen für die Zusammenarbeit der Aufsichtsbehörden verbessert werden können. Darüber hinaus haben die Datenschutzaufsichtsbehörden von Bund und Ländern im vergangenen

Jahr den Arbeitskreis „DSK 2.0“ ins Leben gerufen. Ziel dieses Arbeitskreises ist es, auf Leitungsebene die derzeitige Zusammenarbeit der Aufsichtsbehörden einschließlich der Arbeitsweise der DSK zu evaluieren und weiterzuentwickeln sowie gegebenenfalls Vorschläge für eine Neugestaltung zu erarbeiten. Eine Möglichkeit bestünde aus meiner Sicht darin, eine Institutionalisierung der DSK voranzutreiben. Einhergehend damit müsste geklärt werden, ob und wie analog zum Europäischen Datenschutzausschuss ein ähnliches Gremium auf nationaler Ebene geschaffen und mit entsprechenden Zuständigkeiten ausgestattet werden könnte.

Beratungskompetenz vor Ort ist wichtig

Bedürfnisse der KMU im Blick behalten

Ein weiteres Argument spricht gegen eine Zentralisierung: Die regionale Nähe und die daraus resultierende Beratungskompetenz vor Ort sind einer der wesentlichen Vorteile der föderalen Aufsichtsstruktur. Ich stehe seit meinem Amtsantritt in einem regen Austausch mit niedersächsischen Unternehmen zu Fragen des Datenschutzes. Der Aspekt der Beratung hatte stets eine besondere Bedeutung und hat sie immer noch, weil ich im Rahmen der Umsetzung der DS-GVO rechtlich tragfähige und zugleich praktikable Lösungen finden möchte, und zwar ausgerichtet an den Bedürfnissen und Anforderungen des einzelnen Unternehmens.

Der direkte Kontakt zu den Unternehmen ermöglicht es meiner Behörde, auf Besonderheiten einzugehen. Ich halte es dagegen für sehr fraglich, ob eine zentrale Bundesbehörde als regionaler Ansprechpartner dienen und den heterogenen Bedürfnissen der Wirtschaft gerecht werden kann. Nach meinen Erfahrungen geraten kleine und mittelständische Unternehmen häufig aus dem Blickfeld von Bundesbehörden, so dass die Verwaltungspraxis an Großunternehmen mit den ihnen zur Verfügung stehenden Ressourcen ausgerichtet wird. Dies wäre aber nicht in unserem gemeinsamen Sinne. Die Stärke der Wirtschaft Deutschlands und auch Niedersachsens ist in ihrer bunten Vielfalt begründet und hierbei spielen kleine und mittelständische Unternehmen eine bedeutende Rolle. Eine Landesbehörde kann dieser Vielfalt Rechnung tragen und die kurzen Wege zum allseitigen Vorteil nutzen.

E.2. Bericht aus dem Arbeitskreis Beschäftigtendatenschutz

In der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) führe ich den Vorsitz des Arbeitskreises Beschäftigtendatenschutz (AK BDS). 2020 befasste sich der AK besonders mit der datenschutzrechtlichen Verantwortlichkeit von Personalvertretungen, der Aktualisierung von DSK-Publikationen sowie der Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie.

Ziel des AK BDS ist es, einheitliche Positionen aller Aufsichtsbehörden zu datenschutzrechtlichen Fragen im Beschäftigtenkontext zu erarbeiten. Die turnusmäßige Sitzung des Arbeitskreises im Januar 2020 diente neben dem Erfahrungsaustausch zu Datenschutzüberprüfungen nach der Datenschutz-Grundverordnung (DS-GVO) und zu laufenden Gerichtsverfahren auch der Behandlung von Rechtsfragen zur Umsetzung der DS-GVO.

Ist der Betriebsrat verantwortlich oder nicht?

Im Berichtszeitraum waren insbesondere die Klärung der datenschutzrechtlichen Verantwortlichkeit des Betriebsrats und des Personalrats drängende Fragen. Für die 99. Konferenz der DSK wurden vom Arbeitskreis Beschlussvorlagen erarbeitet, auf deren Basis die DSK den Bundesgesetzgeber schließlich aufforderte, eine gesetzliche Klärung zur Verantwortlichkeit des Betriebsrats in Wahrnehmung seiner Spezifizierungsbefugnis nach Artikel 88 Absatz 1 DS-GVO herbeizuführen. Auf Landesebene gab es entsprechende Vorschläge der Aufsichtsbehörden zur Klärung der Verantwortlichkeit des Personalrats (siehe dazu G.1, S. 60). Ich habe bei den Abstimmungen der DSK stets die Sichtweise vertreten, dass weder der Betriebsrat noch der Personalrat Verantwortlicher im Sinne von Artikel 4 Nummer 7 DS-GVO ist.

Anfang September 2020 wurde die DSK durch den Beirat „Beschäftigtendatenschutz" des Bundesarbeitsministeriums angehört, um den Standpunkt der Aufsichtsbehörden zur Schaffung eines Beschäftigtendatenschutzgesetzes einzuholen. Der AK BDS leistete für die DSK Vorarbeit zu den Leitthemen Entwicklungstrends, Problemfelder und Handlungsbedarfe. Mitglieder des AK nahmen an der Sitzung teil.

Aktualisierte Version des Kurzpapiers Nr. 14: https://t1p.de/kurzpapier-14

Der AK BDS befasste sich im Laufe des Jahres außerdem mit der Aktualisierung von Veröffentlichungen der DSK. So wurde das Kurzpapier Nummer 14 der DSK „Beschäftigtendatenschutz" überarbeitet.
Einen weiteren Schwerpunkt bildete die Verarbeitung von Beschäftigtendaten im Zusammenhang mit der COVID-19-Pandemie, beispielsweise zu Temperaturmessungen oder sonstige Testungen von Beschäftigten (siehe auch J.1.10, S. 121).

E.3. Datenschutzkonferenz fordert verfassungskonforme Registermodernisierung

Die Bundesregierung hat im August 2020 einen Gesetzesentwurf zur Registermodernisierung vorgelegt, um die Datenhaltung der Verwaltungen zu modernisieren und die Digitalisierung voran zu bringen. Ein wesentlicher Bestandteil dieses Gesetzes ist die Einführung einer Identifikationsnummer für alle Bürgerinnen und Bürger.

Bereits 2017 hatte der Normenkontrollrat darauf hingewiesen, dass Deutschland im europäischen Vergleich bei der Digitalisierung der Verwaltung zurückliegt. Zur Verbesserung der Verwaltungsleistungen für Bürgerinnen, Bürger und Unternehmen sowie für den Ausbau digitaler Angebote fordert er die Modernisierung der deutschen Registerlandschaft. In meinem Tätigkeitsbericht 2019 habe ich dazu bereits berichtet. Register enthalten wichtige amtliche Informationen, die eine wesentliche Grundlage für das staatliche Verwaltungshandeln sind.

Tätigkeitsbericht 2019: https://t1p.de/TB2019

Um eine redundante Datenhaltung zu vermeiden und Daten nutzen zu können, die bereits in anderen Verwaltungen vorliegen, strebt die Bundesregierung deren Verknüpfung über die Grenzen einzelner Verwaltungsbereiche hinweg an. Dies soll mithilfe eines eindeutigen Identifiers (auch als Personenkennzeichen bekannt) geschehen. Die Bunderegierung beabsichtigt für diese Verknüpfung auf die bestehende Steuer-Identifikationsnummer (Steuer-ID) zurückzugreifen. Damit löst sich die Steuer-ID allerdings von ihrer ursprünglichen Bestimmung. Die Verwendung der ID wurde bisher nur deshalb als verfassungskonform angesehen, weil sie ausschließlich für rein steuerliche Zwecke verwendet wird.

Datenverwendung auf konkreten Zweck begrenzt

Das Bundesverfassungsgericht hat seit jeher die Verwendung personenbezogener Daten auf den jeweils gesetzlich konkret bestimmten Zweck begrenzt und der Verwendung von Personenkennzeichen enge Schranken auferlegt. Vor diesem Hintergrund hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mehrfach vor der erweiterten Verwendung der Steuer-ID gewarnt. In ihrer Entschließung vom August 2020 hat sie darauf hingewiesen, dass die Schaffung eines solchen einheitlichen und verwaltungsübergreifenden Personenkennzeichens die Gefahr einer umfassenden Profilbildung birgt.

Entschließungen der DSK: https://t1p.de/dsk-entschliessungen

Der Gesetzesentwurf zur Registermodernisierung verknüpft über die Steuer-ID mehr als 50 Register miteinander. Technisch wäre es damit möglich, die Daten zu einer Person aus unterschiedlichen Registern zusammenzuführen. Wenngleich nach dem derzeit geltenden Recht nicht zulässig, könnten etwa theoretisch Daten aus dem Melderegister mit den Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden.

DSK schlägt Alternative vor

Aus Sicht des Datenschutzes ist eine Modernisierung des Verwaltungshandelns begrüßenswert, sie darf allerdings nicht zu Lasten des Datenschutzes betrieben werden. Deshalb hat die DSK ein „sektorspezifisches" Personenkennzeichen vorgeschlagen. Dieses ermöglicht einerseits die eindeutige Identifikation einer Person im Verwaltungsverfahren. Andererseits erschwert es den Missbrauch durch eine datenschutzwidrige Zusammenführung der verteilt vorliegenden Informationen zu einer Person deutlich. Das „sektorspezifische" Modell wird seit vielen Jahren in Österreich erfolgreich betrieben.

Diese Aspekte hat die DSK frühzeitig in die Beratung mit eingebracht. In den entsprechenden Arbeitsgruppen wurden diese jedoch leider nie ernsthaft erwogen und pauschal als zu „komplex" abgelehnt. Die DSK lehnte den Gesetzesentwurf und die zugrunde liegende Architektur ab, da er im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie forderte die Bundesregierung auf, einen verfassungskonformen Entwurf vorzulegen, bevor sie durcheine Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird. Dennoch verabschiedete der Bundestag den Entwurf am 27. Januar 2021. Der Bundesrat stimmte am 5. März 2021 zu.

E.4. Empfehlungen für die digitale Souveränität der öffentlichen Verwaltung

In den Diskussionen um Chancen und Auswirkungen der Digitalisierung tauchen seit Jahren immer wieder die Begriffe „Datensouveränität" und „digitale Souveränität" auf und haben sich fast zu Modebegriffen entwickelt. Wenngleich derzeit noch keine einheitlichen Definitionen existieren, sind diese Begriffe doch klar gegeneinander abzugrenzen.

Bei der Datensouveränität geht es im Kern um eine möglichst weitreichende Kontrolle über die eigenen Daten. Hingegen versteht beispielsweise das „Kompetenzzentrum Öffentliche IT" unter digitaler Souveränität „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können".[1]

Ich habe mich dieser Themen aufgrund ihrer besonderen Tragweite für den Datenschutz frühzeitig angenommen. So hat die Konferenz der unabhängigen Datenschutzbehörden von Bund und Ländern (DSK) während meines Vorsitzes im Jahr 2017 die „Göttinger Erklärung zum Wert des Datenschutzes in der digitalen Gesellschaft" veröffentlicht. Unter dem Eindruck einer bedrohlichen Tendenz zur Verdrängung des Datenschutzes durch eine, wie auch immer geartete Ausprägung der Datensouveränität, hat die DSK sehr deutlich formuliert, dass „die Datensouveränität, […], nur zusätzlich zum Recht auf informationelle Selbstbestimmung greifen, dieses jedoch keinesfalls ersetzen kann." Weiter wird gefordert, dass „die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren nachhaltig gefördert werden muss, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu aufzuwerten.

Genau mit diesem Ziel hat die DSK 2020 mit der Entschließung „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen" weitere Aufklärungsarbeit geleistet und Forderungen an Politik und Verwaltung formuliert.

Entschließungen der DSK: https://t1p.de/dsk-entschliessungen

1 https://t1p.de/oeffentliche-it

IT-Planungsrat greift Thema auch auf

Es freut mich besonders, dass der nationale IT-Planungsrat, das Gremium zur Koordinierung der Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik, ebenfalls das Thema der digitalen Souveränität für die IT der öffentlichen Verwaltung aufgegriffen hat und mit weitreichenden Beschlüssen konsequent vorantreibt. Die fachliche Arbeit dazu erfolgt im Rahmen der eigens dafür ins Leben gerufenen Arbeitsgruppe „Cloud Computing und Digitale Souveränität", in der die DSK durch Mitarbeiterinnen und Mitarbeiter meines Hauses beratend vertreten ist.

Ausgangspunkt für die strategische Zielsetzung des IT-Planungsrates[2] war die durch eine entsprechende Studie[3] untermauerte Feststellung, dass „Verwaltungen für ihre Informations- und Kommunikationstechnik (IKT) Geschäftsbeziehungen mit externen, meist privaten IT-Anbietern aufbauen, die Abhängigkeiten verursachen können. Derartige Abhängigkeiten sind hinsichtlich möglicher Problembereiche zu bewerten, um potentielle Beeinträchtigungen für die Digitale Souveränität der Öffentlichen Verwaltung auszuschließen oder mindestens einzuschränken. Die aktuell identifizierten Problembereiche umfassen

- eingeschränkte Informationssicherheit,
- rechtliche Unsicherheit,
- unkontrollierbare Kosten,
- eingeschränkte Flexibilität und
- fremdgesteuerte Innovation[4]."

Ich betrachte insbesondere den Problembereich der rechtlichen Unsicherheit mit großer Besorgnis. Die DSK hat dazu einstimmig festgestellt, dass „Verantwortliche des öffentlichen Bereichs den Schutz personenbezogener Daten wirkungsvoll umzusetzen haben. Dies kann nur geschehen, wenn sie die Wahlfreiheit und die vollständige Kontrolle über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten haben. Die DSK sieht deshalb die Gewährleistung der digitalen Eigenständigkeit als eines der vordringlichen Handlungsfelder an."

Einsatz von Open-Source-Produkten empfohlen

In der Entschließung „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen" werden wichtige Anforderungen an IT-Produkte aus datenschutzrechtlicher Sicht formuliert und Handlungsempfehlungen zur Umsetzung der strategischen Ziele in der IT der öffentlichen Verwaltung gegeben.

2 31. Sitzung des IT-Planungsrats vom 25. März 2020, Entscheidung 2020/07 - Cloud-Computing und digitale Souveränität

3 Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern
Stand: 23. August 2019 im Auftrag des Bundesministeriums des Innern, für Bau und Heimat

4 https://t1p.de/it-planungsrat

Dabei sind

- datenschutzrechtliche Vorgaben für große Softwareanbieter,
- die in der „Strategischen Marktanalyse“ empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie
- die Nutzung von Open-Source-Software

besonders erfolgversprechende Möglichkeiten.

Der Einsatz von Open-Source-Produkten kann dazu beitragen, die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Software-Anbietern dauerhaft sicherzustellen. Bund, Länder und Kommunen sind dazu aufgefordert, die in der Entschließung aufgeführten Kriterien für eine Stärkung der digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen. Nur unter den genannten Voraussetzungen lassen sich die Grundsätze für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, tatsächlich umsetzen.

Ich bin überzeugt davon, dass sich die konstruktive Zusammenarbeit mit dem IT Planungsrat in diesem strategisch so bedeutsamen Handlungsfeld sinnvoll fortsetzen wird und werde zu gegebener Zeit wieder dazu berichten.

E.5. Deutscher Gesetzgeber immer noch Nachzügler bei der ePrivacy-Regulierung

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat den Bundesgesetzgeber mit einer Entschließung nachdrücklich aufgefordert, endlich die europarechtlichen Verpflichtungen zur Umsetzung der ePrivacy-Richtlinie zu erfüllen und den europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018 fristgemäß umzusetzen. Bereits seit dem Erlass der sogenannten europäischen Cookie-Richtlinie im Jahr 2009 liegt ein nationales Umsetzungsdefizit der europäischen ePrivacy-Regulierung vor. Den Betreiberinnen und Betreibern von Webseiten kann diese Rechtsunsicherheit nicht länger zugemutet werden.

Entschließungen der DSK: https://t1p.de/dsk-entschliessungen

Zwei zeitgleich verlaufende Handlungsstränge veranlassten die DSK, auf der 100. Datenschutzkonferenz am 25. November 2020 die Entschließung „Betreiber von Webseiten benötigen Rechtssicherheit – Bundesgesetzgeber muss europarechtliche Verpflichtungen der ‚ePrivacy-Richtlinie' endlich erfüllen" zu verabschieden.

Erstens hatte der europäische Gesetzgeber am 11. Dezember 2018 die EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation (RL 2018/1972/EU) beschlossen, die von den Mitgliedstaaten bis zum 20. Dezember 2020 umzusetzen war. Ende Juli 2020 war allerdings lediglich ein geleakter Referentenentwurf für ein Telekommunikations-Teledienste-Datenschutzgesetz (TTDSG)[1] in der Öffentlichkeit bekannt geworden. Im Januar 2021 wurde offiziell der Referentenentwurf in die Länder- und Verbandsbeteiligung gegeben. Laut Begründung soll durch dieses Gesetz der europäische Kodex in nationales Gesetz umgesetzt werden. Ob das Gesetz noch in der aktuellen Legislaturperiode erlassen werden wird, ist derzeit nicht absehbar. Es besteht aber schon jetzt eine hohe Wahrscheinlichkeit, dass der europäische Kodex in Deutschland mit wesentlicher Verzögerung in nationales Recht umgesetzt werden wird.

Der zweite Handlungsstrang war die Entscheidung des Bundesgerichtshofs (BGH) vom 28. Mai 2020 zu „Planet49" (siehe Kapitel F.3, S. 57). In dem Urteil nimmt der BGH eine richtlinienkonforme Auslegung von § 15 Abs. 3

1 Der vollständige Gesetzestitel lautet „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der elektronischen Kommunikation und bei Telemedien sowie zur Änderung des Telekommunikationsgesetzes, des Telemediengesetzes und weiterer Gesetze".

Telemediengesetz (TMG) vor, um diesen anschließend als europarechtskonforme Umsetzung von Art. 5 Abs. 3 ePrivacy-RL bewerten zu können. Die Tatsache, dass die vorgenommene Auslegung die Grenzen des Wortlauts der Norm deutlich überschreitet, führt das bisher bestehende Umsetzungsdefizit deutlich vor Augen. Zudem geht der BGH davon aus, dass § 15 Abs. 3 TMG unter Zugrundlegung der europarechtskonformen Auslegung neben den Vorschriften der Datenschutz-Grundverordnung (DS-GVO) anwendbar sei. Die Entscheidung des BGH bestätigt, dass die in § 15 Abs. 3 TMG formulierte Widerspruchslösung keine europarechtskonforme Umsetzung von Art. 5 Abs. 3 ePrivacy-RL darstellt. Es wird ausdrücklich festgestellt, dass Betreiberinnen und Betreiber von Webseiten Cookies zur Erstellung von Nutzungsprofilen für Zwecke der Werbung oder Marktforschung nur mit Einwilligung des Nutzers oder der Nutzerin einsetzen dürfen.

Cookies nur mit Einwilligung der Nutzerinnen und Nutzer

Divergierende Auffassungen von DSK und BGH

Diese Anwendung des europarechtskonform ausgelegten § 15 Abs. 3 TMG steht im Widerspruch zur der bereits im April 2018 von der DSK veröffentlichten Positionsbestimmung „Zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018". Die DSK vertritt den Standpunkt, dass die Datenschutzvorschriften des Telemediengesetzes (§§ 11 ff. TMG) neben der DS-GVO nicht mehr anwendbar sind. Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht. Allein die Tatsache, dass die nationalen Datenschutzaufsichtsbehörden und das deutsche Zivilgericht der höchsten Instanz zu einer sehr praxisrelevanten Rechtsfrage divergierende Auffassungen vertreten, verdeutlicht das Ausmaß der Rechtsunklarheit.

Der deutsche Gesetzgeber plant, das seit mehr als elf Jahren bestehende Umsetzungsdefizit in Bezug auf Art. 5 Abs. 3 ePrivacy-RL durch den Erlass eines Telekommunikations-Telemedien-Datenschutzgesetzes zu beheben. Durch diese Gesetz soll zudem der europäische Kodex für elektronische Kommunikation in nationales Recht umgesetzt werden. Allerdings liegt auch hier bereits ein europarechtlicher Verstoß vor, da die Umsetzungsfrist bis zum 20.12.2020 nicht eingehalten und der Erlass eines Umsetzungsgesetzes nicht absehbar ist.

Vor allem Webseitenbetreiberinnen und -betreiber sowie andere Akteure, die Adressaten der europäischen ePrivacy-Regulierung sind, brauchen für Ihre Dienste u. a. in Bezug auf „Cookies" Rechtsklarheit und -sicherheit. Anderenfalls ist eine datenschutzkonforme Gestaltung kaum möglich. Zugleich ist es mir bei einer derart unklaren Rechtslage kaum möglich, die mir durch die DS-GVO übertragene Aufgabe, die Anwendung der Datenschutzgesetze zu überwachen und durchsetzen, angemessen zu erfüllen. Aus diesen Gründen habe ich mich dafür eingesetzt, dass die DSK den Gesetzgeber mit einer Entschließung auffordert, bestehende Rechtsunsicherheiten umgehend durch eine klare und europarechtskonforme Gesetzgebung unter Berücksichtigung der DS-GVO zu beseitigen.

Anbieter brauchen Rechtssicherheit

E.6. Entschließung für eine vertrauenswürdige Ende-zu-Ende-Verschlüsselung

Nach dem Terroranschlag von Wien im November 2020 haben Polizei und Geheimdienste erneut gefordert, den unmittelbaren Zugriff auf verschlüsselte Kommunikationsinhalte von Messenger-Diensten zu gewähren. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern (DSK) hat diese Pläne in einer Entschließung kritisiert.

Entschließungen der DSK: https://t1p.de/dsk-entschliessungen

Im Zuge der Kriminalitäts- und Terrorismusbekämpfung scheint eine durchgehende Verschlüsselung von Kommunikation, wie sie zum Teil von Messengern angeboten wird, unerwünscht zu sein. Denn mit dem Wegfall der Ende-zu-Ende-Verschlüsselung würden die Sicherheitsbehörden Zugang zu den Kommunikationsinhalten und damit ein, so sagen sie, wichtiges Instrument zur Aufklärung und Verhinderung von Straftaten und besonders von Terroranschlägen erhalten. Nach dem Resolutionsentwurf „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" des Rates der Europäischen Union[1] sollen entsprechende Möglichkeiten in Zusammenarbeit mit den Anbietern von Online-Diensten wie WhatsApp, Threema oder Signal entwickelt werden. Dies könnte das komplette Aus für eine effektive Ende-zu-Ende-Verschlüsselung bedeuten.

In ihrer 100. Konferenz hat die DSK am 25. November 2020 die Entschließung „Für eine vertrauenswürdige Ende-zu-Ende-Verschlüsselung – Pläne des EU-Rates stoppen" verabschiedet. Damit wird den Forderungen entgegengetreten, Sicherheitsbehörden und Geheimdiensten den Zugriff auf bislang verschlüsselte Kommunikationsinhalte zu eröffnen. Auch ich habe wiederholt eindringlich auf die Bedeutung einer Ende-zu-Ende Verschlüsselung zur Wahrung der Vertraulichkeit der elektronischen Kommunikation hingewiesen.

Eine starke Verschlüsselung ist eine der zentralen Voraussetzungen für die grundrechtlich durch das Fernmeldegeheimnis gewährleistete Vertraulichkeit von Individualkommunikation und das Vertrauen in diese Kommunikationsformen. Das Prinzip der Verschlüsselung hat sich als ein wesentlicher Baustein zur Garantie der Vertraulichkeit der Kommunikation bewährt und wird in der Datenschutz-Grundverordnung (DS-GVO) ausdrücklich als Maßnahme zur Sicherheit der Verarbeitung hervorgehoben. Die Verschlüsselung gehört zu

1 Nummer 12143/1/20 vom 6. November 2020.

den herausgehobenen Bausteinen eines „Datenschutzes durch Technikgestaltung“ („Privacy by Design“) und hilft damit, die Anforderungen der DS-GVO zum Schutz der Betroffenen wirksam umzusetzen.

Verschlüsselungsverbot beeinträchtigt Grundrechte

Ein Verschlüsselungsverbot beeinträchtigt die Grundrechte, wie sie etwa in Artikel 8 der Europäischen Menschenrechtskonvention, der Charta der Grundrechte der Europäischen Union sowie im deutschen Grundgesetz verankert sind. Zu rechtfertigen wären derartig schwere Eingriffe allenfalls dann, wenn sie aufgrund ihrer Eignung, Erforderlichkeit und Angemessenheit als unabweisbar betrachtet werden müssten. Die Beschlussvorlage des Rates der EU liefert hierfür jedoch keine schlüssigen Belege und wird von der DSK daher abgelehnt.

Sowohl die Wirtschaft und Verwaltung als auch die Bürgerinnen und Bürger müssen im Rahmen der Digitalisierung auf eine sichere Ende-zu-Ende-Verschlüsselung vertrauen können. Auch die Ziele des Online-Zugangsgesetzes, Verwaltungsleistungen elektronisch über Portale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten.

Zudem empfiehlt der Europäische Datenschutzausschuss als Reaktion auf das „Schrems II“-Urteil des Europäischen Gerichtshofs die Verschlüsselung als zentrales Mittel der technisch-organisatorischen Maßnahmen zur Gewährleistung des EU-Schutzniveaus für die Datenübermittlung in Drittländer.

Zwar ist das angestrebte Ziel, die Ermittlungsmöglichkeiten von Sicherheitsbehörden nachhaltig und effektiv zu verbessern, nachzuvollziehen. Dafür ist aber ein Aufbrechen der Ende-zu-Ende-Verschlüsselung nicht erforderlich. Die Sicherheitsbehörden verfügen bereits über entsprechende Mittel wie die Quellen-Telekommunikationsüberwachung, machen aber davon kaum Gebrauch.

E.7. Datenschutzkonferenz veröffentlicht neue Bewertung von Google Analytics

Google Analytics ist eines der am weitesten verbreiteten Werkzeuge für Webseiten-Betreiber, mit dessen Hilfe sich umfassende statistische Auswertungen der Seitennutzung vornehmen lassen. Die Datenschutzaufsichtsbehörden haben den Einsatz von Google Analytics mit Blick auf die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) neu bewertet.

Pressemitteilung zu Google Analytics: https://t1p.de/lfd-analytics

Bis zur Geltung der DS-GVO waren die Aufsichtsbehörden davon ausgegangen, dass Google Analytics ohne eine datenschutzrechtliche Einwilligung der Nutzerinnen und Nutzer eingesetzt werden kann, sofern bestimmte Voraussetzungen erfüllt worden sind. Allerdings ist einerseits das Tool technisch weiterentwickelt worden, anderseits hat sich die Rechtslage durch die Geltung der DS-GVO verändert. Zahlreiche Aufsichtsbehörden hatten bereits in einer Pressemeldung vom 14. November 2019 klargestellt, dass Google Analytics und ähnliche Dienste nur mit Einwilligung zulässig sind.

In den am 12. Mai 2020 veröffentlichten Hinweisen zum Einsatz von Google Analytics im nicht-öffentlichen Bereich hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern (DSK) die Mindestanforderungen für den datenschutzkonformen Einsatz beschrieben. Diese Hinweise ergänzen die Orientierungshilfe für Anbieter von Telemedien.

Die rechtliche Bewertung kommt zu zwei neuen Erkenntnissen:

Hinweise der DSK: https://t1p.de/dsk-analytics

- Google und der Google-Analytics-Anwender sind gemeinsam für die Datenverarbeitung verantwortlich, sodass die Anforderungen des Art. 26 DS-GVO zu beachten sind. Die bisherige Bewertung, dass beim Einsatz von Google Analytics eine Auftragsverarbeitung anzunehmen ist, ist somit überholt.

- Ein rechtmäßiger Einsatz von Google Analytics ist in der Regel nur aufgrund einer wirksamen Einwilligung der Nutzerinnen und Nutzer der Webseite gem. Art. 6 Abs. 1 lit. a), i.V.m. Art. 7 DS-GVO möglich. Bisher wurde dem Nutzer oder der Nutzerin ein Widerspruchsrecht eingeräumt.

Sofern Betreiber von Webseiten Google Analytics einsetzen, müssen sie mindestens die folgenden spezifischen Maßnahmen umsetzen:

Das müssen Anbieter von Webseiten umsetzen

- Einholung einer informierten, freiwilligen, aktiven und vorherigen Einwilligung der Nutzerinnen und Nutzer
- Technische Implementierung eines einfachen und immer zugänglichen Mechanismus (z. B. Schaltfläche) zum Widerruf der einmal vom Nutzer oder der Nutzerin erteilten Einwilligung auf der Webseite
- Bereitstellung und jederzeitige Abrufbarkeit umfassender Informationen über die Verarbeitung personenbezogener Daten im Rahmen von Google Analytics

Darüber hinaus sollte der für Google Analytics bereitgestellte Befehl zur Kürzung der IP-Adressen der Nutzerinnen und Nutzer in den Code der Webseite übernommen werden.

Hinweise sind keine Empfehlung zur Verwendung

Die Neubewertung des Einsatzes von Google Analytics war sehr wichtig. Die DS-GVO verfolgt neben dem Datenschutz von Betroffenen das Ziel, den europäischen Binnenmarkt gerade in Bezug auf die digitale Wirtschaft zu fördern. Daher war die Klarstellung erforderlich, dass für den Einsatz von Google Analytics dieselben datenschutzrechtlichen Anforderungen gelten wie für andere Analyse-Tools und insgesamt für auf Webseiten eingebundene Drittdienste. Ich möchte betonen, dass die Hinweise zum Einsatz von Google Analytics nicht als Empfehlung für dessen Einsatz missverstanden werden dürfen. Es werden zahlreiche Analyse-Tools auch von europäischen Unternehmen angeboten, die dieselben Funktionen aufweisen, darunter auch einige Dienste, die die datenschutzrechtlichen Grundsätze Privacy by Design und Privacy by Default beherzigen.

Über die genannten grundsätzlichen datenschutzrechtlichen Bedenken hinaus, gilt es zu beachten, dass beim Einsatz von Google Analytics Nutzerdaten in die USA übermittelt werden. Dies ist seit der Entscheidung zu Schrems-II (siehe Seite 27) ein weiteres Hemmnis für einen datenschutzkonformen Einsatz des Analyse-Tools.

E.8. Auftragsverarbeitung bei Microsoft Office 365

Ich erhalte regelmäßig Anfragen von Verantwortlichen, wie Produkte von Microsoft datenschutzkonform eingesetzt werden können. Aufgrund der schieren Größe der Produktpalette von Microsoft und deren rascher Weiterentwicklung sowie wegen der vertraglichen Rahmenbedingungen können Bewertungen aus datenschutzrechtlicher Sicht immer nur sehr gezielt und punktuell abgegeben werden. Im Jahr 2020 habe ich mich sehr intensiv mit der Bewertung der Auftragsverarbeitung bei Office 365 auseinandergesetzt.

Tätigkeitsbericht 2019: https://t1p.de/TB2019

Wie bereits in meinem Tätigkeitsbericht für 2019 beschrieben, hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern (DSK) einen Arbeitskreis zur datenschutzrechtlichen Bewertung der Auftragsverarbeitung beim Einsatz von Office 365 in der Cloud eingesetzt. Gegenüber früheren Office-Versionen werden in 365 ausschließlich Online-Versionen von Word, Outlook, OneNote, PowerPoint, Excel und OneDrive zur Verfügung gestellt, so dass die Datenverarbeitung in der Cloud erfolgt.

Strategie auf die Cloud ausgerichtet

Alle Landesdatenschutzbeauftragten wurden von Anwenderinnen und Anwendern mit Fragen zum datenschutzkonformen Einsatz von Office 365 konfrontiert. Die Verunsicherung war nachvollziehbar, da die Datenverarbeitung in einer Cloud viele Fragen zu Datensicherheit und Datenschutz aufwirft. Aktiv beworben werden jedoch meist nur die kaufmännischen Vorteile für die Kundinnen und Kunden, wie zum Beispiel günstigere Betriebskosten, flexible Abnahmemengen oder auch die hohe Betriebsstabilität. Die Gesamtstrategie von Microsoft zielt darauf ab, die Kundinnen und Kunden weg von lokalen Installationen („on premise“) hin zu cloudbasierten Services zu bewegen. So werden zukünftig die Office-Produkte viel stärker als bisher nur noch als „Service“ angeboten („Software as a Service“ - SaaS), was mit deutlichen Vorteilen für die Wartungsfreundlichkeit und die Release-Strategie einhergehen kann. Andererseits hat dies aber auch erhebliche Auswirkungen auf die Beherrschbarkeit der Risiken für die Privatsphäre der Nutzerinnen und Nutzer. Grund genug also, die Rahmenbedingungen, unter denen derartige Produkte in der Cloud angeboten werden, sorgfältig zu überprüfen.

Defizite im Dialog benannt

Ein maßgebliches Ziel der Arbeit der Datenschutzbeauftragten ist es, für Rechtssicherheit für Verantwortliche zu sorgen und tatsächliche Verbesserungen im Datenschutz für die Betroffenen herbeizuführen. Daher war es meinen Kolleginnen und Kollegen und mir ein wichtiges Anliegen, Vertreter der Firma Microsoft von Anfang an in die Arbeiten des Arbeitskreises mit einzubeziehen. Im Dialog wurden die erkannten Defizite benannt und nach

Möglichkeiten gesucht, die Anforderungen der Datenschutz-Grundverordnung (DS-GVO), vor allem die Bestimmungen zur Auftragsverarbeitung gemäß Art. 28 DS-GVO, mit den standardisierten Vereinbarungen von Microsoft (Online Service Terms und Data Processing Agreement) in Einklang zu bringen.

Positiv anzumerken ist, dass Microsoft die Gesprächsangebote des Arbeitskreises aktiv aufgegriffen, sich intensiv an den Erörterungen auf Fachebene beteiligt und eine zielgerichtete Weiterentwicklung der Online Service Terms in Aussicht gestellt hat. Bereits in einer Sondersitzung der DSK im Herbst 2019 kündigten Julie Brill, Corporate Vice President und stellvertretende General Counsel für Datenschutz bei Microsoft und ihre Delegation eine Neufassung der Online Service Terms für ganz Europa an. Im Ergebnis wurden Anfang 2020 revidierte Online Service Terms veröffentlicht, in deren Neufassung die Empfehlungen des Arbeitskreises teils aufgegriffen worden, teils jedoch auch unberücksichtigt geblieben sind.

Trotz Verbesserungen bleiben Mängel

Gemäß Art. 28 DS-GVO muss es Auftraggebern möglich sein, sowohl Art und Zweck der Verarbeitung als auch die Art der personenbezogenen Daten näher zu beschreiben und zu konkretisieren. Dies betrifft insbesondere die Beschreibung im Falle der Verarbeitung besonderer Kategorien personenbezogener Daten, bspw. zu rassischer und ethnischer Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, genetischen Daten, biometrischen Daten oder auch Gesundheitsdaten. Dieser Anforderung genügen die neu gefassten Online Service Terms mit Stand vom Januar 2020 jedoch weiterhin nicht.

Zudem verweist Microsoft innerhalb der Datenschutzbestimmungen für Microsoft Online-Dienste (Data Processing Agreement – DPA) auf Folgendes: Soweit das Unternehmen personenbezogene Daten im Zusammenhang mit eigenen „legitimen Geschäftstätigkeiten" verwendet oder anderweitig verarbeitet, sei Microsoft als ein unabhängiger Datenverantwortlicher für diese Verwendung und für die Einhaltung aller geltenden Gesetze sowie die Erfüllung der Verpflichtungen verantwortlich. Es ist jedoch nicht eindeutig ersichtlich, was Microsoft als „legitime Geschäftstätigkeit" definiert und welche weiteren personenbezogenen Daten hier verarbeitet werden sollen.

Anforderungen der DS-GVO nicht erfüllt

Aufgrund dieser verbliebenen (und weiterer) Defizite in den Online Service Terms und dem Data Processing Agreement stellte der Arbeitskreis der DSK fest, dass der Einsatz von Office 365 in Bezug auf die Auftragsverarbeitung nicht den Anforderungen der DS-GVO entspricht. Die DSK folgte der Feststellung des Arbeitskreises und setzte Microsoft offiziell über die datenschutzrechtliche Bewertung der Auftragsverarbeitung bei Office 365 in Kenntnis.

Dialog mit Microsoft wird fortgesetzt

Für Anwenderinnen und Anwender, Verantwortliche und Aufsichtsbehörden ist die Situation angesichts der immer noch verbliebenen rechtlichen Unsicherheiten unbefriedigend und kann so nicht hingenommen werden. Daher hat die DSK den Arbeitskreis beauftragt, erneut mit Microsoft in Gespräche zu gehen und dabei neben weiteren erforderlichen Verbesserungen in den Online Service Terms auch offene Fragen zur Verarbeitung von Telemetriedaten und den Rechtsgrundlagen beim Datentransfer in die USA zu erörtern sowie datenschutzkonforme Lösungen zu finden.

Insofern kann ich die Festlegung der Datenschutzkonferenz zur Auftragsverarbeitung unter Office 365 noch immer nur als einen Zwischenstand im Gesamtkontext der datenschutzrechtlichen Fragestellungen betrachten. Ich bin jedoch zuversichtlich, dass die Datenschutzkonferenz im Dialog mit Microsoft mit Nachdruck für die erforderlichen Nachbesserungen eintreten wird.

E.9. Akkreditierung und Zertifizierung

Die Datenschutz-Grundverordnung (DS-GVO) bietet Prüfverfahren zur datenschutzrechtlichen Zertifizierung von Verarbeitungstätigkeiten an. Auf diese Weise können Verantwortliche sich offiziell bestätigen lassen, dass personenbezogene Daten datenschutzkonform verarbeitet werden. Hierzu haben die Aufsichtsbehörden des Bundes und der Länder im Jahr 2020 zwei Grundlagenpapiere finalisiert. Meine Erwartung ist es, dass die Zertifizierung von Herstellern und Anbietern aktiv als Bestandteil der Geschäfts- und Marketingstrategie erkannt und genutzt werden wird.

Mit den Artikeln 42 und 43 der DS-GVO hat der Gesetzgeber einen rechtlichen Grundstein für EU-weit einheitliche Akkreditierungs- und Zertifizierungsverfahren geschaffen, um die Einhaltung der DS-GVO bei Verarbeitungsvorgängen nachzuweisen. Mit der freiwilligen Zertifizierung nach Art. 42 DS-GVO kann nachgewiesen werden, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird.

Zertifizierung soll Vertrauen der Beteiligten stärken

Das Ziel der Zertifizierung besteht darin, allen Beteiligten Vertrauen darin zu geben, dass ein Produkt, Prozess oder eine Dienstleistung Anforderungen der DS-GVO erfüllt. Als explizite Anwendungsbereiche, bei denen eine Zertifizierung für den Nachweis der Einhaltung der Grundverordnung als Faktor herangezogen werden kann, nennt die DS-GVO beispielsweise:

- die Erfüllung der Anforderungen an Technikgestaltung und datenschutz-freundliche Voreinstellungen des Art. 25 Abs. 1 und 2 (vgl. Abs. 3) und
- die Sicherheit der Verarbeitung (Art. 32 Abs. 3).

Allerdings hebt Art. 42 Abs. 4 DS-GVO hervor, dass eine erfolgreiche Zertifizierung eine Organisation nicht von der Verantwortung für die Einhaltung der DS-GVO befreit. Ein nach DS-GVO genehmigtes Zertifikat kann jedoch bei aufsichtsrechtlichen Kontrollen von Vorteil sein und die Prüfung erleichtern.

Damit eine Zertifizierungsstelle tätig sein darf, muss sie sich vorab akkreditieren lassen. Im Rahmen des Verfahrens nach Art. 42 und Art. 43 DS-GVO sind sowohl die Deutsche Akkreditierungsstelle (DAkkS) als auch die Datenschutzaufsichtsbehörden für die Akkreditierung von Zertifizierungsstellen gemeinsam tätig. Gemäß § 39 Bundesdatenschutzgesetz (BDSG) erfolgt die Erteilung der Befugnis, als Zertifizierungsstelle tätig zu werden, durch die zuständige Aufsichtsbehörde des Bundes oder der Länder. Bei erfolgreicher Akkreditierung nach Art. 42 Abs. 5 DS-GVO können die Zertifizierungsstellen eine Datenschutz-Zertifizierung nach der DS-GVO erteilen.

Konzeptpapiere der Aufsichtsbehörden

Die Aufsichtsbehörden des Bundes und der Länder haben sich auf eine gemeinsame Vorgehensweise verständigt und Konzeptpapiere zu Akkreditierungs- und Zertifizierungsverfahren entwickelt.

Die Stellen, die im Datenschutzbereich zertifizieren möchten, werden durch die DAkkS zusammen mit der zuständigen Aufsichtsbehörde akkreditiert. Interessierte Stellen müssen dabei sowohl die Anforderungen der EN-ISO/IEC 17065/2012 erfüllen als auch ergänzende Anforderungen aus dem Datenschutzbereich, die im Papier „Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065" beschrieben sind. In dieser ISO-Norm werden Anforderungen an die Zertifizierungsstellen definiert, wie beispielsweise die Unparteilichkeit, finanzielle Unabhängigkeit und Vertraulichkeit der Zertifizierungsstelle. Das Anforderungspapier wurde zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzausschuss abgestimmt und ist nun Maßstab für Stellen, die eine Akkreditierung anstreben.

Anwendungshinweise der Datenschutzkonferenz: https://t1p.de/dsk-anwendung

Um die Zusammenarbeit bei der Akkreditierung zwischen den einzelnen Aufsichtsbehörden des Bundes und der Länder untereinander und mit der DAkkS zu regeln, wurde eine Kooperationsvereinbarung getroffen. In dieser Vereinbarung sind allgemeine Regelungen über die Zusammenarbeit vereinbart, einschließlich der Bereitstellung von Fachpersonal durch die Aufsichtsbehörden. Die Aufsichtsbehörden unterstützen sich freiwillig bei der Stellung von Fachpersonal.

Der eigentlichen Akkreditierung ist eine Programmprüfung vorgeschaltet, die gemeinsam von der DAkkS und der zuständigen Aufsichtsbehörde durchgeführt wird. In der Norm EN-ISO/IEC 17067/2013 sind die grundsätzlichen Anforderungen an diese Prüfung enthalten. Diese allgemeinen Anforderungen werden noch um datenschutzspezifische Anforderungen für Programme der Konformitätsbewertung ergänzt (Dokument „Anforderungen an Zertifizierungsprogramme"). Durch dieses gemeinsame Dokument der deutschen Aufsichtsbehörden wird die Prüfung über Landesgrenzen weiter vereinheitlicht und ein bundesweiter Standard geschaffen.

Ablaufschema des Akkreditierungsprozesses: https://t1p.de/Akkreditierungsprozess

Durch die Digitalisierung sowie die weiter zunehmende Bedeutung von Cloud-Lösungen und verteilten Infrastrukturen nimmt die Komplexität von Verarbeitungstätigkeiten ständig zu. Daher begrüße ich den Ansatz der Zertifizierung von Verarbeitungstätigkeiten als wichtige vertrauensbildende Maßnahme. Sie schafft Transparenz und Sicherheit sowohl für verantwortliche Stellen als auch für Nutzerinnen und Nutzer.

F. Rechtsprechung von grundsätzlicher Bedeutung

F.1. EuGH bleibt bei Vorratsdatenspeicherung seiner Linie treu

Urteil des EuGH:
https://t1p.de/eugh-vds

Am 6. Oktober 2020 hat der Europäische Gerichtshof (EuGH) erneut ein Urteil zur Vorratsdatenspeicherung gefällt, in dem er seine Grundsatzentscheidung aus dem Jahr 2014 bestätigt. Er hält daran fest, dass eine anlass- und unterschiedslose Speicherung von Kommunikationsdaten auf Vorrat für die Zwecke der allgemeinen Verbrechensbekämpfung oder zur Wahrung der nationalen Sicherheit gegen europäisches Recht verstößt.

Mit dem Begriff Vorratsdatenspeicherung wird das vor allem von Strafverfolgungsbehörden und Geheimdiensten immer wieder beschworene Instrument beschrieben, dass Anbieter von Telekommunikationsdiensten ohne Anlass und Differenzierung verpflichtet werden sollen, personenbezogene Kommunikationsdaten über ihre Kundinnen und Kunden für längere Zeiträume zu speichern und zur Ermittlung und Verfolgung von Straftaten zur Verfügung zu stellen.

Hintergrund der neuerlichen EuGH-Entscheidung waren drei Gerichtsverfahren, die in Frankreich und Belgien geführt wurden. Die nationalen Verfahren betrafen nationalstaatliche Regelungen, nach denen Anbieter elektronischer Kommunikationsdienste verpflichtet werden, die Verkehrs- und Standortdaten der Nutzerinnen und Nutzer an eine Behörde weiterzuleiten bzw. diese Daten allgemein oder anlasslos aufzubewahren. Die Vorschriften betreffen nicht die Kommunikationsinhalte, sondern die die sogenannten Metadaten. Aber auch aus diesen Informationen, wer, wie lange, mit wem und wie oft kommuniziert hat, lassen sich bereits Rückschlüsse auf die Inhalte der Kommunikation ziehen. In diesen Verfahren stellten die Gerichte jeweils Vorlagefragen an den EuGH, die teils deckungsgleich, teils unterschiedlich waren.

Kernaussagen der EuGH-Entscheidung

Der EuGH stellte zunächst ausdrücklich fest, dass die ePrivacy-RL (Richtlinie über Datenschutz und elektronische Kommunikation) auf die im Streit stehen-

den nationalen Rechtsvorschriften anwendbar ist. Von den Mitgliedstaaten wurde teilweise argumentiert, dass die Regelungen nicht in den Anwendungsbereich der ePrivacy-RL fallen würden. Denn der Zweck dieser Rechtsvorschriften bestehe darin, die nationale Sicherheit zu gewährleisten, die in der alleinigen Verantwortung der Mitgliedstaaten liege.

Anschließend betonte der EuGH, dass die ePrivacy-RL den Mitgliedstaaten nicht erlaubt, weitreichende gesetzliche Ausnahmen von der grundsätzlichen Verpflichtung zu normieren, die Vertraulichkeit der elektronischen Kommunikation zu gewährleisten. Die Ausnahmeregelungen der Mitgliedstaaten dürfen nicht dazu führen, dass das durch die ePrivacy-RL vorgegebene Regel-Ausnahme-Verhältnis ins Gegenteil verkehrt wird. Eine Einführung der Vorratsdatenspeicherung in den Mitgliedstaaten muss den allgemeinen Grundsätzen des EU-Rechts, einschließlich des Grundsatzes der Verhältnismäßigkeit, und den durch die Charta garantierten Grundrechten entsprechen. Diesen europarechtlichen Anforderungen entsprachen die nationalstaatlichen Vorschriften zur Vorratsdatenspeicherung nicht. Mitgliedstaatliche Regelungen, die Anbieter von Telekommunikationsdaten zur wahllosen und anlasslosen Speicherung von Kommunikationsdaten verpflichten, sind ausgeschlossen. Dies gilt erst recht, wenn darüber hinaus eine grundsätzliche Pflicht zur Übermittlung der gespeicherten Daten an Sicherheits- und Geheimdienste vorgesehen ist.

Keine wahl- und anlasslose Speicherung von Kommunikationsdaten

Anforderungen an den Datenzugriff

Umgekehrt traf der EuGH auch Aussagen dazu, welche nationalstaatlichen Regelungen im Zusammenhang mit der Datennutzung von elektronischen Kommunikationsdiensten möglich wären. Aus den verschiedenen im Urteil dargestellten Fällen, lassen sich vor allem die folgenden grundsätzlichen Anforderungen für eine europarechtskonforme Regelung ableiten:

- Vorliegen einer ernsthaften Bedrohung der nationalen Sicherheit
- Die Maßnahme muss zeitlich auf das unbedingt Notwendige begrenzt sein.
- Die Anordnung gegenüber dem Anbieter von elektronischen Kommunikationsdiensten muss vorab durch ein Gericht oder eine unabhängige Verwaltungsstelle überprüft werden.

Anordnung der Speicherung unter engen Voraussetzungen möglich

- Der Rückgriff auf die gespeicherten Daten muss auf Grundlage objektiver und nichtdiskriminierender Faktoren nach den Kategorien der betroffenen Personen oder unter Verwendung eines geografischen Kriteriums begrenzt sein.
- Die allgemeine und wahllose Aufbewahrung von IP-Adressen, die der Quelle einer Mitteilung zugewiesen sind, setzt voraus, dass die Aufbewahrungsfrist auf einen unbedingt erforderlichen Zeitraum beschränkt ist.

Als zulässig werden auch Vorschriften angesehen, durch die der Rückgriff auf von Telekommunikationsdienstleistern zu anderen Zwecken gespeicherten Daten beschleunigt wird. Auch in diesem Fall forderte der EuGH, dass die Maßnahme erforderlich ist, um schwerwiegende Straftaten zu beleuchten oder Angriffe auf die nationale Sicherheit.

Der Zugriff auf die Echtzeiterfassung von Verkehrs- und Standortdaten kann nur gesetzlich legitimiert werden, wenn sie sich nur auf Personen bezieht und vorher durch ein Gericht bestätigt worden ist.

Aus für die Vorratsdatenspeicherung in Deutschland?

Die Politik wird nicht müde, die Vorratsdatenspeicherung immer wieder als unverzichtbares Element für Strafverfolgungsbehörden und Geheimdienste anzuführen. Auch in Deutschland ist die im Telekommunikationsgesetz seit 2015 erneut vorgesehene Vorratsdatenspeicherung aufgrund eines Klageverfahrens vor dem Bundesverwaltungsgericht aktuell nur ausgesetzt. Der EuGH muss auch zu § 113a Abs. 1 i.V.m. § 113b TKG noch eine Entscheidung treffen. Die Entscheidungen zu den Vorschriften aus Frankreich und Belgien lassen vermuten, dass die deutschen Vorschriften zur Vorratsdatenspeicherung nicht mit dem Europarecht vereinbar sind.

F.2. Anwendung der Datenschutz-Grundverordnung auf Parlamente

Nach einem Urteil des Europäischen Gerichtshofs (EuGH) vom 9. Juli 2020 haben Bürger gegenüber dem Petitionsausschuss eines Landtags ein Recht auf Auskunft nach Art. 15 Datenschutz-Grundverordnung (DS-GVO). Diese Entscheidung wirkt zunächst recht unscheinbar. Ihre mögliche Tragweite offenbart sich erst bei einem zweiten Blick. Denn aufgrund des Urteils drängt sich die Frage auf, ob die DS-GVO auch allgemein im Kernbereich der parlamentarischen Willensbildung Geltung beanspruchen kann.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte sich bereits kurz nach Geltungsbeginn der DS-GVO mit der Grundsatzfrage befasst, in welchem Verhältnis diese zur Arbeit im Bereich von Parlamenten, Fraktionen, Abgeordneten und politischen Parteien steht. Die DSK war in ihrem Beschluss vom 5. September 2018 zu dem Ergebnis gelangt, dass die DS-GVO auf Datenverarbeitungen von Parlamenten, einschließlich deren Organen sowie Abgeordneten, keine Anwendung findet, soweit diese den parlamentarischen Kerntätigkeiten zuzuordnen sind. Diese Sichtweise stützt sich im Wesentlichen darauf, dass die DS-GVO keine Anwendung auf Tätigkeiten findet, die nicht in den Anwendungsbereich des Unionsrechts fallen (Art. 2 Abs. 2 Buchstabe a DS-GVO).

Beschlüsse der DSK: https://t1p.de/dsk-beschluesse

Auskunftsanspruch gegenüber dem Hessischen Landtag

Die vermeintlich geklärte Grundsatzfrage bekam erneut praktische Relevanz, als ein Petent vom Hessischen Landtag nach Art. 15 DS-GVO Auskunft über die über ihn beim Petitionsausschuss gespeicherten personenbezogenen Daten begehrte. Dieser Auskunftsantrag wurde vom Landtagspräsidenten mit der Begründung abgelehnt, dass das Petitionsverfahren eine parlamentarische Aufgabe des Hessischen Landtags darstelle, welche nicht im Geltungsbereich der DS-GVO liege. Der Petent verfolgte sein Auskunftsbegehren daraufhin per Klage weiter. Das angerufene Verwaltungsgericht Wiesbaden setzte das Verfahren aus und legte dem EuGH die Frage vor, ob die DS-GVO auf den für die Bearbeitung von Bürgereingaben zuständigen Ausschuss eines Parlaments eines Mitgliedstaats Anwendung finde, insbesondere, ob es sich bei dem Petitionsausschuss um eine „Behörde" im Sinne von Art. 4 Nr. 7 DS-GVO handele.[1]

1 VG Wiesbaden, Beschluss vom 28.03.2019 – 6 K 1016/15.

EuGH: Petitionsausschüsse unterliegen der DS-GVO

Mit Urteil vom 9. Juli 2020 entschied der EuGH, dass ein Petitionsausschuss als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO anzusehen sei und dessen Verarbeitung personenbezogener Daten in den Anwendungsbereich der DS-GVO falle. Somit sei auch Art. 15 DS-GVO anwendbar.[2] Nach Ansicht des EuGH müsste die Ausnahme vom sachlichen Anwendungsbereich für Tätigkeiten, die nicht dem Anwendungsbereich des Unionsrechts unterliegen, eng ausgelegt werden. Eine Ausnahme vom Anwendungsbereich gelte nur für Tätigkeiten, die ausdrücklich in Art. 2 Abs. 2 DS-GVO genannt würden, was auf die Tätigkeiten des Petitionsausschusses nicht zutreffe. Ebenso wenig seien im 20. Erwägungsgrund und in Art. 23 DS-GVO Ausnahmen in Bezug auf parlamentarische Tätigkeiten vorgesehen.

DSK berät über Folgen des EuGH-Urteils

Die Ausführungen des EuGH beziehen sich unmittelbar nur auf nationale Petitionsausschüsse. Gleichwohl stellt sich die Frage, ob aus diesem Urteil darüber hinaus abzuleiten ist, dass die DS-GVO auf Datenverarbeitungen von Parlamenten Anwendung findet, auch soweit deren parlamentarische Kerntätigkeit betroffen ist. Einerseits könnte man bei Petitionsausschüssen durchaus eine Sonderrolle annehmen, weil diese nur mittelbar zur parlamentarischen Tätigkeit beitragen und deren Tätigkeiten vielfach administrativer Natur sind. Andererseits dürfte sich die Argumentation des EuGH zum sachlichen Anwendungsbereich der DS-GVO auch auf die parlamentarischen Kerntätigkeiten von Parlamenten übertragen lassen. Über diese Grundsatzfrage wird daher erneut innerhalb der DSK beraten. Bis zur Klärung hat die DSK ihren Beschluss vom 5. September 2018 zunächst ausgesetzt.

2 EuGH, Urteil vom 09.07.2020 – Rs. C-272/19.

F.3. BGH-Entscheidung: Weiterhin keine Rechtsklarheit für Cookies auf Webseiten

Der Bundesgerichtshof (BGH) hat im Verfahren des Bundesverbandes der Verbraucherzentralen (VZBV) gegen die als Adresshändlerin und Gewinnspielbetreiberin tätige Planet49 GmbH eine mit Spannung erwartete Entscheidung in Bezug auf Cookies auf Webseiten gefällt. Zum einen stellte er fest, dass § 15 Abs. 3 Telemediengesetz neben der Datenschutz-Grundverordnung (DS-GVO) anwendbar sei. Zum anderen entschied der Gerichtshof, dass ein voreingestelltes Ankreuzkästchen im Cookie-Fenster einer Webseite keine wirksame datenschutzrechtliche Einwilligung darstelle.

Der Entscheidung des BGH ging ein Vorabentscheidungsverfahren vor dem Europäischen Gerichtshof (EuGH) voraus, in dem bereits im Vorjahr eine Entscheidung ergangen war (siehe meinen Tätigkeitsbericht 2019).
Der EuGH hatte am 1. Oktober 2019 geurteilt, dass keine wirksame Einwilligung vorliegt, wenn die Speicherung von oder der Zugriff auf Informationen, die bereits im Endgerät des Nutzers oder der Nutzerin einer Webseite gespeichert sind, mittels Cookies durch ein voreingestelltes Ankreuzkästchen erlaubt wird, das zur Verweigerung der Einwilligung abgewählt werden muss.[1] Der BGH folgte nun wenig überraschend dieser Vorabentscheidung.[2]

Tätigkeitsbericht 2019: https://t1p.de/TB2019

Sehr bemerkenswert ist allerdings der Weg, den der BGH gewählt hat, um zu diesem Ergebnis zu gelangen. Der BGH legt in seiner Entscheidung § 15 Abs. 3 TMG mit dem Ziel einer europarechtskonformen Umsetzung von Art. 5 Abs. 3 ePrivacy-Richtlinie aus und nimmt an, dass schon im Fehlen einer wirksamen Einwilligung ein im Telemediengesetz genannter Widerspruch gesehen werden könne und deshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Ausdeutung von § 15 Abs. 3 TMG wendet er diese Vorschrift neben der DS-GVO an.

Widerspruch zur Rechtsauffassung der DSK

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte erstmals in der Entschließung vom 5. Februar 2015 „Keine Cookies ohne Einwilligung der Internetnutzer“ auf die fehlende

Entschließungen der DSK: https://t1p.de/dsk-entschliessungen

1 EuGH, MMR 2019, 732, Rn. 57.
2 BGH, MMR 2020, 609, Rn. 52.

Umsetzung von Art. 5 Abs. 3 ePrivacy-RL hingewiesen und den Gesetzgeber zum Handeln aufgefordert. Wiederholt wurde diese Forderung in der Positionsbestimmung der DSK vom 26. April 2018 zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018 sowie der Orientierungshilfe für Anbieter von Telemedien mit Stand vom März 2019. Verstärkt wurde die bereits bestehende Rechtsunsicherheit durch die fehlende Anpassung der nationalen Datenschutzvorschriften im Telemediengesetz. Um für verantwortliche Stellen eine Linie vorzugeben, teilte die DSK in der genannten Positionsbestimmung frühzeitig mit, dass die Vorschriften der §§ 11 ff. TMG aufgrund des Anwendungsvorrangs der DS-GVO nicht mehr anwendbar sind. Der BGH hat nun zumindest in Bezug auf § 15 Abs. 3 TMG eine gegenteilige Entscheidung getroffen.

Bewertung des BGH-Urteils

Auch wenn die Entscheidung des BGH im Ergebnis zu begrüßen ist, ist sie rechtsdogmatisch nur schwer nachvollziehbar. Erstens werden die Grenzen einer zulässigen Auslegung von Vorschriften massiv überdehnt, indem das im Wortlaut vorgesehene Widerspruchsrechts (Opt Out) zu einem Einwilligungserfordernis (Opt In) umgedeutet wird. Zweitens ergeben sich dadurch starke Zweifel, ob § 15 Abs. 3 TMG noch dem verfassungsrechtlichen Bestimmtheitsgrundsatz entspricht.

BGH-Urteil lässt viele Fragen offen

Schwerer wiegen für die Aufsichtspraxis allerdings die zahlreichen offenen Fragen im Zusammenspiel zwischen Art. 5 Abs. 3 ePrivacy-RL und § 15 Abs. 3 TMG, die durch den BGH nicht beantwortet worden sind, weil es sich um eine Einzelfallentscheidung handelte:

- Wie können die unterschiedlichen Anwendungsbereiche der DS-GVO einerseits und der ePrivacy-RL andererseits unter Berücksichtigung von § 15 Abs. 3 TMG voneinander abgegrenzt werden?
- Soll der europarechtskonform ausgelegte § 15 Abs. 3 TMG unabhängig davon gelten, ob in einem Cookie personenbezogene Daten enthalten sind?
- Soll der europarechtskonform ausgelegte § 15 Abs. 3 TMG auch gelten, wenn ohne den Einsatz von Cookies eine Speicherung von Informationen oder ein Zugriff auf Informationen erfolgt, die im Endgerät eines Nutzers oder einer Nutzerin gespeichert sind?
- Soll der europarechtskonform ausgelegte § 15 Abs. 3 TMG auch gelten, wenn die Cookies nicht zur Erstellung von Nutzerprofilen für Zwecke der Werbung oder Marktforschung dienen, sondern z.B. für die bedarfsgerechte Gestaltung,[3] die technische Umsetzung der Webseite, die Speicherung des Einwilligungsstatus des Nutzers bzw. der Nutzerin oder wenn keine Nutzerprofile erstellt werden?
- Welche Ausnahmeregelungen gelten von dem grundsätzlichen Einwilligungserfordernis oder anders gefragt, welche Cookies können datenschutzkonform ohne Einwilligung der Nutzerinnen und Nutzer eingesetzt werden?
- Sind außer § 15 Abs. 3 TMG auch die weiteren Datenschutzvorschriften des Telemediengesetzes, die §§ 11 ff. TMG, neben der DS-GVO anwendbar?
- Welcher Bußgeldrahmen gilt für einen Verstoß gegen das Einwilligungserfordernis?

3 Unklar ist auch, ob die dritte Zweckvariante der bedarfsgerechten Gestaltung in § 15 Abs. 3 TMG lediglich in Bezug auf den Streitfall nicht relevant eingestuft worden ist oder generell für diese Cookies – vermutlich mit Blick auf die Ausnahmen von Art. 5 Abs. 3 ePrivacy-RL – nicht genannt worden sind.

Rechtsunsicherheit bleibt

Klargestellt wurde durch die Entscheidung, dass für den Einsatz von Cookies und anderen Tracking-Technologien eine datenschutzrechtliche Einwilligung erforderlich ist, die den Anforderungen gem. Art. 4 Nr. 11 und Art. 7 DS-GVO entsprechen muss. Im Umfeld dieser Kernaussage verbleibt allerdings sehr viel Rechtsunsicherheit, die nicht durch Gerichte oder die Aufsichtsbehörde, sondern allein durch den Gesetzgeber beseitigt werden kann. Die Cookie-Entscheidungen des EuGH aus 2019 und des BGH aus 2020 haben bereits zu einer deutlichen Verbesserung des Cookie-Einsatzes auf den Webseiten geführt. Es bleibt zu hoffen, dass der Gesetzgeber diese positive Entwicklung zeitnah durch eine umfassende Regelung mit Blick auf die Rechte der Betroffenen weiter fördert.

G. Beteiligung an Gesetzgebungsverfahren

G.1. Beteiligung an Gesetzgebungsverfahren im Überblick

Im Berichtszeitraum war meine Behörde an 18 Gesetzgebungsverfahren, 10 Verordnungsentwürfen sowie weiteren Erlassen und Verwaltungsvorschriften der Landesregierung beteiligt. Dies betraf die gesamte Bandbreite der Tätigkeit der Landesregierung. Dabei haben mir die meisten Ressorts im Rahmen der Verbandsbeteiligung eine Gelegenheit zur datenschutzrechtlichen Stellungnahme eingeräumt. Diese Vorgehensweise trägt den rechtlichen Vorgaben zwar Rechnung. Gleichwohl würde eine frühzeitigere Einbindung meiner Behörde im Rahmen der Erstellung des Referentenentwurfs oder der Ressortbeteiligung eine stärkere Berücksichtigung datenschutzrechtlicher Aspekte ermöglichen.

Beteiligung der LfD Niedersachsen an Gesetzgebungs- und Verordnungsverfahren:

Gesetze:

- Gesetzentwurf zur Durchführung der Verordnung (EU) 2019 816 sowie zur Änderung weiterer Vorschriften
- Entwurf eines Gesetzes zur Verbesserung des Schutzes von Gerichtsvollzieherinnen und Gerichtsvollziehern vor Gewalt sowie zur Änderung weiterer zwangsvollstreckungsrechtlicher Vorschriften
- Kirchensteuerrahmengesetz
- Niedersächsisches Gleichberechtigungsgesetz
- Niedersächsisches Ausführungsgesetz zum Zensusgesetz 2021
- Gesetz zur Ausübung des Hebammenberufs
- Niedersächsisches Pflegegesetz
- Änderung des Gesetzes über das Klinische Krebsregister Niedersachsen
- Bestattungsgesetz
- Niedersächsisches Gesetz über den öffentlichen Gesundheitsdienst

- Niedersächsisches Maßregelvollzugsgesetz
- Änderung des Niedersächsischen Hochschulgesetzes
- Gesetz zur Neugestaltung des niedersächsischen Rechts der Tageseinrichtungen für Kinder und der Kindertagespflege
- Niedersächsisches Wohnraumförderungsgesetz
- Gesetz zur Umsetzung der Auflösung der Pflegekammer
- Kammergesetz für die Heilberufe
- Gesetz zur Änderung des Niedersächsischen Architektengesetzes, des Niedersächsischen Ingenieurgesetzes und der Niedersächsischen Bauordnung
- Gesetz zur Änderung des Niedersächsisches Landeswahlgesetzes und des Niedersächsisches Kommunalwahlgesetzes

Verordnungen:

- Entwurf einer Verordnung des Justizministeriums zur elektronischen Aktenführung bei Gericht
- Allgemeine Gebührenordnung
- Verordnung über die Ausbildung und Prüfung für den allgemeinen Verwaltungsdienst in den Laufbahnen der Fachrichtung Allgemeine Dienste
- Verordnung über die Wahl zur Kammerversammlung Landwirtschaftskammer Niedersachsen
- Niedersächsische Verordnung über den Vorschuss auf Dienstbezüge bei Urlaub zur Betreuung, Pflege oder Begleitung
- Verordnung zur Änderung der klinischen Krebsregister Niedersachsen - Datenschutzbestimmungsverordnung
- Verordnung über die Berufsbildenden Schulen
- Düngeverordnung Nitrat u Phosphat
- Niedersächsische Meldedatenverordnung
- Spielordnung für die öffentlichen Spielbanken in Niedersachsen

Leider gibt es auch immer wieder Gesetzgebungsverfahren, in die meine Behörde gar nicht eingebunden wird. Dabei wird oftmals wohl verkannt, dass rechtliche Vorgaben fast immer auch mit einer Verarbeitung personenbezogener Daten einhergehen, für die es normenklarer Regelungen bedarf. Auch nach Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) gilt für Datenverarbeitungen weiterhin das Verbot mit Erlaubnisvorbehalt. Im Mai 2020 hat das Bundesverfassungsgericht erneut ausgeführt, dass Eingriffe in das Recht auf informationelle Selbstbestimmung wie jede Grundrechtsbeschränkung stets einer gesetzlichen Ermächtigung bedürfen, die einen legitimen Gemeinwohlzweck verfolgt und im Übrigen den Grundsatz der Verhältnismäßigkeit wahren müssen.[1]

Änderung im Personalvertretungsgesetz angeregt

Ein Beispiel, bei dem ich aktiv an Legislative und Exekutive herangetreten bin, um eine unklare Rechtslage zu klären, ergab sich 2020 im Kontext des Beschäftigtendatenschutzes. Ich habe sowohl gegenüber dem Niedersächsischen Landtag als auch gegenüber dem Niedersächsischen Ministerium für Inneres und Sport angeregt, bei der Änderung des Niedersächsischen Personalvertretungsgesetzes (NPersVG) eine normenklare Regelung zur Verantwortlichkeit des Personalrats, der Jugend- und Ausbildungsvertretungen sowie der Einigungsstelle im Sinne der DS-GVO aufzunehmen. Diese Anregung ist leider bisher nicht umgesetzt worden. Ich wäre dankbar, wenn mein Vorschlag, dass weder der Personalrat noch andere personalvertretungsrechtliche Gremien Verantwortliche im Sinne von Artikel 4 Nummer 7 DS-GVO sind, in zukünftigen Gesetzgebungsverfahren zur Änderung des NPersVG Berücksichtigung finden würde. Denn würden Personalvertretungen ebenfalls als Verantwortliche betrachtet, müssten sie alle datenschutzrechtlich vorgegebenen Pflichten erfüllen wie die öffentliche Stelle, der sie angehören.

1 Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13

G.2. Änderung des Bundesmeldegesetzes

Das Zweite Gesetz zur Änderung des Bundesmeldegesetzes wurde im Berichtszeitraum in den Bundestag eingebracht. Zu diesem Gesetz habe ich gegenüber dem zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in einer Stellungnahme Bedenken mitgeteilt.

Im Gesetzesentwurf wird § 39 a neu eingefügt, durch den eine Meldebehörde die Möglichkeit bekommt, Betroffenendaten, die sie durch eine elektronische Anfrage einer anderen öffentlichen Stelle erhält, automatisiert auf Übereinstimmung mit den im Melderegister gespeicherten Daten zu prüfen. Stimmen die Daten mit den im Melderegister gespeicherten Daten überein, bestätigt die Meldebehörde dies der anfragenden öffentlichen Stelle. Eine gleichlautende Regelung enthält der neu geplante § 49 a für Anfragen, die von sonstigen Stellen gestellt werden.

Die damit einhergehende mögliche Ausweitung von automatisierten Abrufen halte ich für bedenklich. Zudem wurde in der Gesetzesbegründung zu diesen automatisierten Bestätigungen ausgeführt, dass es sich hierbei nicht um eine Übermittlung, sondern nur um eine Bestätigung der Übereinstimmung handeln würde. Dieses Verständnis ist aus datenschutzrechtlicher Sicht nicht nachvollziehbar. Vielmehr stellt auch eine Bestätigung bzw. Nichtbestätigung ein personenbezogenes Datum dar, bezogen auf die Aktualität und Richtigkeit. Daher läge auch eine Übermittlung vor.

Gesetzesbegründung ist nicht nachvollziehbar

Vor diesem Hintergrund sehe ich die Ausweitung der automatisierten Übermittlungen kritisch. In das parlamentarische Verfahren hat meine Kritik allerdings keinen Eingang gefunden. Gegen Ende 2020 wurden die genannten Änderungsregelungen vom Bundestag mit Zustimmung des Bundesrats beschlossen.

H. Aufklärung und Öffentlichkeitsarbeit

H.1. Vorträge der Landesdatenschutzbeauftragten

Wie fast alles im vergangenen Jahr hat sich auch meine Vortragstätigkeit wegen der Corona-Pandemie grundlegend verändert. Denn ab März waren verständlicherweise keine Live-Veranstaltungen mehr möglich. Stattdessen standen nun – nach einer kurzen Phase des Innehaltens – Online-Vorträge und Hybrid-Konferenzen auf dem Programm. Trotz Pandemie nahm ich 2020 mehr als 30 solcher Termine wahr.

Allein im Büro statt im Konferenzsaal

Die meistbenutzten Einstiegsworte für Vorträge waren im vergangenen Jahr nicht „meine sehr geehrten Damen und Herren…", sondern „können Sie mich hören?". Kam auf diese Frage keine Antwort, folgten die hektische Suche nach Einstellungsmöglichkeiten und der Wechsel von Lautsprecher auf Headset – oder umgekehrt. Vor allem in den ersten Wochen der Online-Veranstaltungen war es sehr ungewohnt, nicht mehr vor einem vollbesetzten Konferenzsaal zu sprechen, sondern allein im Büro vor dem Monitor zu sitzen. Doch es war mir auch in diesem so ungewöhnlichen Jahr wichtig, zu informieren, zu sensibilisieren und meine Behörde nach außen zu vertreten.

Themen werden spezifischer

Bußgeldpraxis der Aufsichtsbehörden

Waren 2018 und 2019 vor allem noch die Vorträge in der Mehrzahl, die sich allgemein mit den Änderungen und Anforderungen der Datenschutz-Grundverordnung (DS-GVO) auseinandersetzten, wurden die Themen im vergangenen Jahr deutlich spezifischer. Auf großes Interesse stieß zum Beispiel wenig überraschend die Bußgeldpraxis der Datenschutzaufsichtsbehörden. In den Jahren zuvor war die Diskussion über dieses Thema eher eine theoretische, doch inzwischen hatte ich ausreichend Erfahrungen mit Bußgeldern nach der DS-GVO gesammelt, um einen praktischen Einblick in die Sanktionspraxis meiner Behörde geben zu können (siehe auch I.4, S. 81). Überhaupt waren wie schon in den vergangenen Jahren besonders Akteure aus der Wirtschaft interessiert daran, wie ich meine Rolle als Aufsichtsbehörde ausfülle. Unter anderem habe ich mit Unterstützung der Unternehmerverbände Niedersachsen Vorträge für mehrere regionale Arbeitgebervertretungen gehalten.

Ebenfalls sehr gefragt waren Ausführungen zum ersten Evaluationsbericht der EU-Kommission zur DS-GVO, zu den allgemeinen Entwicklungen auf europäischer Ebene (darunter auch die E-Privacy-Verordnung) und zu den Auswirkungen des Schrems II-Urteils auf den internationalen Datenverkehr (siehe auch D.1, S. 27).

Homeoffice und Videokonferenzen

Zwei Themen, die mit Beginn der ersten Pandemie-Welle eine enorme Konjunktur erlebten, waren der Datenschutz im Homeoffice im Allgemeinen und die datenschutzrechtlichen Anforderungen an Videokonferenzen im Speziellen. Zu beiden Fragestellungen habe ich auch zügig Informationsmaterial auf meiner Webseite veröffentlicht (siehe H.3, S. 67).

Auch 2021 steht bislang unter keinen guten Vorzeichen für Live-Veranstaltungen. Dennoch hoffe ich, dass es bald wieder möglich sein wird, sich persönlich auszutauschen. Denn so sehr Online-Konferenzen in den vergangenen Monaten zur Routine geworden sind, können sie doch Begegnungen von Angesicht zu Angesicht in keiner Weise ersetzen.

H.2. Datenschutz geht zur Schule

Nachdem die erste Beteiligung meiner Behörde an der Aktion „Datenschutz geht zur Schule“ ein voller Erfolg war, besuchten meine Mitarbeiterinnen und Mitarbeiter auch 2020 Schulen in Niedersachsen, um Jugendliche für einen bewussten Umgang mit Internet und sozialen Medien zu sensibilisieren. Ich arbeitete dabei erneut mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD), der die Aktion 2009 ins Leben gerufen hatte.

Initiative des BvD: https://t1p.de/datenschutz-schule

Rund um den „Safer Internet Day“ am 11. Februar 2020 suchten meine Mitarbeiterinnen und Mitarbeiter acht Schulen in Celle, Göttingen, Hameln, Hannover, Hildesheim, Lüneburg, Osnabrück und Wolfenbüttel auf. Dabei erreichten sie rund 1200 Schülerinnen und Schüler der siebten und achten Klassen und sprachen unter anderem darüber, was ein sicheres Passwort ausmacht, was Jugendliche vor einem Posting in sozialen Medien bedenken sollten und wie man sich als Opfer von Cybermobbing verhalten kann.

Nach den vielen positiven Rückmeldungen des vorangegangenen Jahres war ich sehr erfreut darüber, dass sich erneut zahlreiche engagierte Beschäftigte meines Hauses freiwillig als Referentinnen und Referenten anboten. Denn mit „Datenschutz geht zur Schule“ treten wir in den direkten Dialog mit Schülerinnen, Schülern und Lehrkräften und holen die Jugendlichen in ihrer unmittelbaren Lebensrealität ab.
In ihren Vorträgen griffen die Referentinnen und Referenten wieder auf das Material des BvD zurück, der auch ein Handbuch für Lehrkräfte kostenlos zur Verfügung stellt.

Ich hätte den BvD auch 2021 gerne wieder unterstützt, doch die Corona-Pandemie machte es unmöglich, in den Schulen vor Ort zu sein. Zwar habe ich eine digitale Alternative geprüft, bin aber zu dem Schluss gekommen, dass sie für diese Art des Austauschs nicht geeignet wäre. Wir werden die Aktionswoche aber nachholen, sobald es die Lage wieder zulässt.

H.3. Veröffentlichung von Informationsmaterial

Ein nach wie vor bedeutender Aspekt meiner Arbeit besteht darin, Informationsmaterialien zu verschiedensten Bereichen des Datenschutzes zu veröffentlichen. Auf diese Weise sollen Verantwortliche, Auftragsverarbeiter und Betroffene sensibilisiert und aufgeklärt werden. Einige Publikationen wurden 2020 thematisch von der Corona-Pandemie diktiert, aber längst nicht alle.

Mit dem ersten Lockdown im Frühjahr 2020 und der Notwendigkeit im Homeoffice zu arbeiten, nahmen auch die diesbezüglichen Anfragen an mich zu. Viele Unternehmen, freiberuflich Tätige, Selbstständige und Behörden hatten sich zwar bereits auch schon vor Pandemie gefragt, wie sie die Arbeit von zu Hause datenschutzkonform gestalten können. Die Dringlichkeit nahm aber nun deutlich zu. Ich veröffentlichte deshalb Hinweise zum Umgang mit personenbezogenen Daten bei der Arbeit im Homeoffice.

Datenschutz im Homeoffice: https://t1p.de/ds-homeoffice

Häufige Fragen zu Videokonferenzen

Ebenfalls stark im öffentlichen Fokus standen die datenschutzrechtlichen Anforderungen an Videokonferenzsysteme, da diese zwangsläufig von zahlreichen Beschäftigten, Schülerinnen und Schülern sowie Studierenden genutzt werden mussten. Verantwortliche Stellen sehen sich bei der Auswahl des passenden Systems einer grundsätzlichen Herausforderung gegenüber: Während die Datenschutz-Grundverordnung (DS-GVO) von ihnen verlangt, Datenschutz schon bei der Produktauswahl (Privacy by Design) und in den Voreinstellungen dieser Produkte (Privacy by Default) angemessen zu berücksichtigen, gelten diese Verpflichtungen bedauerlicherweise nicht für die Produkthersteller und Diensteanbieter. Umso wichtiger war es mir, Hinweise zur Auswahl datenschutzfreundlicher Angebote und zur praktischen Durchführung von Videokonferenzen zu geben.

FAQ zu Videokonferenzen: https://t1p.de/ds-videokonferenz

Unterstützung bei der Kontakterfassung

Ab Anfang Mai 2020 mussten zahlreiche Branchen und Einrichtungen die Kontaktdaten von Kunden und Kundinnen, Besucherinnen und Besuchern sowie Teilnehmenden erfassen, wenn diese die Geschäftsräume oder Einrichtungen betreten bzw. an einer Veranstaltung teilnehmen wollen (siehe J.1.1, S. 102). Dies wurde in der Niedersächsischen Corona-Verordnung festgeschrieben und sollte die Gesundheitsämter im Fall einer Corona-Infektion bei der Nachverfolgung von Kontakten unterstützen. Viele der von dieser Pflicht

Hinweise und Muster zur Datenerhebung: https://t1p.de/corona-daten

betroffenen Stellen waren zunächst mit der datenschutzkonformen Umsetzung der Kontakterfassung überfordert. Ich habe deshalb Hinweise und Muster auf meiner Webseite veröffentlicht und dies unter anderem bei Wirtschaftsverbänden und Berufskammern bekannt gemacht. Auch für Sportvereine veröffentlichte ich ähnliche Hinweise.

Consent-Banner richtig gestalten

Hinweise für die Anforderungen an Consent-Layer: https://t1p.de/consent-layer

Ohne Bezug zu Corona, aber deshalb nicht weniger wichtig war meine Handreichung für datenschutzkonforme Einwilligungen auf Webseiten, die Anforderungen an sogenannte Consent-Layer formulierte. Sowohl für die Verwendung von Cookies als auch generell für die Einbindung von Drittdienstleistern auf ist eine datenschutzrechtliche Einwilligung der Nutzer erforderlich. Vor der Geltung der DS-GVO wurden überwiegend einfache Cookie-Banner auf Webseiten eingesetzt, durch die Nutzerinnen und Nutzer in der Regel über den Einsatz von Cookies lediglich informiert wurden. Mittlerweile finden sich vermehrt aufwändige Consent-Fenster (auch Banner oder Layer genannt), die detaillierte Informationen über den Einsatz von Cookies und Drittdiensten sowie echte Wahlmöglichkeiten bieten. Entsprechend aufwändiger sind ihre Gestaltung und Umsetzung geworden.

FAQ zu Dashcams, Auftragsverarbeitung und Betriebsräten

Übersicht der FAQ: https://t1p.de/faq-uebersicht

Weiterhin veröffentlichte ich im Lauf des Jahres mehrere FAQ, in denen häufig gestellte Fragen zu verschiedenen Bereichen des Datenschutzes beantwortet werden. Dies betraf etwa Dashcams im Straßenverkehr, deren unsachgemäßer Einsatz auch mit einem Bußgeld geahndet werden kann (siehe I.4, S. 81). Darüber hinaus beantwortete ich Fragen zur datenschutzrechtlichen Position von Betriebsräten sowie zur Auftragsverarbeitung gemäß Artikel 28 DS-GVO. Um die Informationsmaterialien meiner Behörde besser auffindbar zu machen, entschied ich mich zudem dafür, meine Webseite um eine zentrale „Infothek“ zu erweitern.

H.4. Datenschutzkompetenz für Digitalisierungsprojekte

Die Digitalisierung spielt in Wirtschaft, Verwaltung und Gesellschaft eine zunehmend größere Rolle. Die Konferenz der unabhängigen Datenschutzbeauftragten von Bund und Ländern (DSK) fordert deshalb, die Entwicklung datenschutzkonformer IT-Produkte und -Verfahren nachhaltig zu fördern, um den Datenschutz zu einem Qualitätsmerkmal der europäischen Digitalwirtschaft zu machen. Meine Mitarbeiterinnen und Mitarbeiter unterstützen in diesem Sinne die Sensibilisierung und Steigerung der Datenschutzkompetenz bei den verantwortlichen Stellen.

Es gilt, sich frühzeitig mit den Vorteilen aber auch den Risiken der Digitalisierung auseinander zu setzen und sie transparent zu machen. Die DSK fordert dazu auf, den hohen Wert des Rechts auf informationelle Selbstbestimmung für eine freiheitliche Gesellschaft zu achten und sich nachdrücklich vertrauensbildend für die Persönlichkeitsrechte einzusetzen.

Digitalisierung ist ein wesentlicher Schwerpunkt der Politik der niedersächsischen Landesregierung. Die Strategie Niedersachsens zur digitalen Transformation wurde 2018 in einem Masterplan beschrieben. Dabei werden sowohl die Wirtschaft als auch die Verwaltung adressiert. Ein wesentlicher Erfolgsfaktor der Digitalisierung ist die Akzeptanz der Nutzerinnen und Nutzer durch Vertrauen in die Sicherheit und Vertraulichkeit der verarbeiteten Daten zu gewährleisten.

Keine Digitalisierung ohne Datenschutz

Schulungen zum technisch-organisatorischen Datenschutz

Um die Digitalisierungsoffensive an dieser Stelle zu unterstützen, haben Beschäftigte meines Hauses auch im Jahr 2020 wieder Seminare insbesondere für die Projektleiter und -verantwortlichen der Masterplanprojekte angeboten. Diese halbtägigen Seminare vermitteln die Grundlagen des technisch-organisatorischen Datenschutzes und der Datenschutz-Folgenabschätzung (DSFA). Leitend ist dabei der Gedanke, die Datenschutzkompetenz frühzeitig in die Digitalisierungsprojekte einzubringen, um bereits von Beginn an Datenschutz zu berücksichtigen. So ist der Datenschutz bereits bei der Konzepterstellung und der Architekturentscheidungen mitzudenken, um dem Prinzip „Data Protection By Design“ Rechnung tragen zu können.

Ein weiteres, wichtiges Handlungsfeld ist die Umsetzung von Projekten zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen nach dem Online-Zugangs-Gesetz (OZG). Da die OZG Umsetzungsprojekte in den deutschen

Bundesländern die Anwendungen nach dem „Eine-für Alle“ Prinzip[1] bereitstellen wollen, hat die DSK eine koordinierte, aktive Beteiligung durch ihre Mitglieder beschlossen. Sie wird im Jahr 2021 eine Praxishilfe zur Verfügung stellen, die die Anforderungen an eine datenschutzrechtliche Dokumentation für eine vereinfachte Nachnutzbarkeit[2] der Anwendungen aus dem OZG-Leistungskatalog beschreibt.

Niedersachsen für Gesundheit zuständig

Niedersachsen hat im Rahmen der Bund-Länder Zusammenarbeit die Federführung für das Themenfeld Gesundheit. Das bedeutet, dass in Niedersachsen diese Leistungen zentral entwickelt und betrieben werden, um anschließend anderen Ländern und Kommunen zur Verfügung zu stehen, und gegebenenfalls nur geringfügig angepasst werden müssen.

Im Vorgriff auf diese Initiative hat mein Haus in einem weiteren Seminar bereits Projektverantwortliche aus unterschiedlichen Behörden zur Durchführung einer DSFA geschult. Die für die Umsetzung der OZG-Projekte verantwortlichen Bediensteten sollten frühzeitig über die datenschutzrechtlichen Anforderungen informiert werden, um diese bereits bei der Verfahrensentwicklung berücksichtigen zu können. Gerade bei der Umsetzung von OZG-Projekten werden verstärkt innovative Technologien und neue organisatorische Lösungen eingesetzt. Die damit einhergehenden Risiken für den Datenschutz lassen sich nur im Rahmen einer qualifizierten DSFA angemessen bewerten und verringern.

Unterstützung der Digitalagentur Niedersachsen

Um neben der Unterstützung der niedersächsischen Verwaltung auch die Wirtschaft mit Aufklärungsangeboten zu erreichen, kooperiere ich mit der Digitalagentur Niedersachsen. In der Digitalagentur werden u. a. die Beratungsangebote zur digitalen Transformation mit Wirtschaft und Forschung in Niedersachsen koordiniert. Im Rahmen der regelmäßigen Sitzungen des Arbeitskreises IT-Security haben Beschäftigte meiner Behörde den Prozess zur Auswahl angemessener Sicherungsmaßnahmen (ZAWAS) präsentiert. Dieser Prozess wurde durch mein Haus entwickelt, um die verantwortlichen Stellen bei der Auswahl angemessener Sicherungsmaßnahmen zu unterstützen. Auf Grund des großen Interesses an dem Prozess ZAWAS sind weitere gemeinsame Veranstaltungen geplant.

1 Das bedeutet, dass ein Land oder eine Allianz aus mehreren Ländern eine Leistung zentral entwickelt und betreibt und diese anschließend anderen Ländern und Kommunen zur Verfügung stellt, die den Dienst dann geringfügig lokal anpassen müssen.

2 Nachnutzung bedeutet, dass die Arbeitsergebnisse der Themenfelder sowie bereits digitalisierte Leistungen anderen Ländern und Kommunen zur Verfügung gestellt werden, die an der Umsetzung nicht unmittelbar beteiligt waren. Sie müssen somit nur einen Bruchteil der OZG-Leistungen selbst digitalisieren.

I. Aufsicht und Vollzug

I.1. Zahlen und Fakten

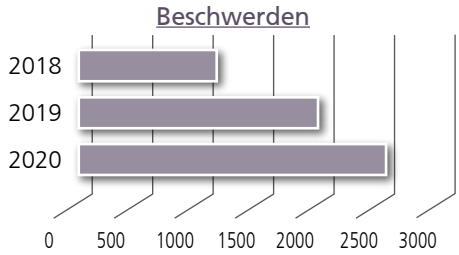
Um einen schnellen Überblick über die Arbeit meiner Behörde zu ermöglichen, veröffentliche ich an dieser Stelle ausgewählte statistische Werte und Kennzahlen. Dies soll dazu beitragen, meine Tätigkeit transparent zu machen. Allerdings ist damit keine Aussage über die qualitative Ausprägung der hier aufgeführten Aufgabenbereiche getroffen.

Beratungen

Im Jahr 2020 erreichten mich rund 1600 schriftliche Beratungsanfragen (per Post oder E-Mail). Zwar ist die Beratung im Einzelfall nicht als meine gesetzliche Aufgabe festgelegt. Dennoch bemühen sich meine Mitarbeiterinnen und Mitarbeiter nach Kräften, Unterstützung zu leisten. Bedauerlicherweise ist das aber aufgrund der angespannten Personalsituation in meinem Haus nicht immer möglich.

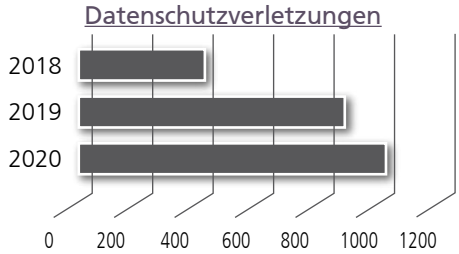
Beschwerden

Die Zahl der Beschwerden, die Betroffene gemäß Art. 77 DS-GVO bei der Aufsichtsbehörde einreichen können, ist im vergangenen Jahr erneut deutlich gestiegen. Gingen 2018 bereits etwas mehr als 1000 Beschwerden ein, weil sich die Betroffenen in ihren Rechten verletzt sahen, waren es 2019 insgesamt 1882 und 2020 schon 2479.



Gemeldete Datenschutzverletzungen

Auch die gemäß Art. 33 DS-GVO gemeldeten Datenschutzverletzungen nahmen im vergangenen Jahr weiter zu. Nach 370 Meldungen 2018 und 824 im Jahr 2019 waren es diesmal insgesamt 989.



Abhilfemaßnahmen nach DS-GVO

Ich habe 2020 vor allem in Bezug auf die Verwarnungen deutlich stärker von meinen Abhilfebefugnissen gem. Art. 58 Abs. 2 DS-GVO Gebrauch gemacht als im Jahr zuvor. So habe ich 4 Warnungen (Art. 58, Abs. 2 lit.a DS-GVO), 17 Anweisungen und Anordnungen (Art. 58, Abs. 2 lit. c-g und j) sowie 381 Verwarnungen (Art. 58, Abs. 2 lit.b DS-GVO) ausgesprochen.

Zudem habe ich 28 Bußgeldbescheide erlassen (siehe I.4, S. 81). Die Gesamthöhe der verhängten Bußgelder betrug 10,56 Millionen Euro (2019: 480.000 Euro).

Europäische Verfahren

Im Jahr 2020 war mein Haus in folgendem Umfang mit europäischen Verfahren befasst:

1. Verfahren mit Betroffenheit (Art. 56): 325
2. Verfahren mit Federführung (Art. 56): 5
3. Verfahrensschritte gem. Kap VII DS-GVO (Art. 60 ff.):
   a. Die LfD hat als betroffene Aufsichtsbehörde einen Beschlussentwurf erhalten: 72 Fälle
      Die LfD hat als betroffene Aufsichtsbehörde einen überarbeiteten Beschlussentwurf erhalten: 12 Fälle
   b. Der LfD wurde als betroffener Aufsichtsbehörde ein finaler Beschlussentwurf vorgelegt: 32 Fälle
   c. Verfahren mit Federführung (Art. 60): 3 Fälle

Ressourcen der Behörde

Jahr	Budget in Tsd. Euro	Beschäftigungsvolumen
2017	3.581	45,25
2018	3.917	50,25
2019	4.117	51,17
2020	4.271	53,17

I.2. Beschwerden und Meldungen von Datenschutzverletzungen

Seit der Geltung der Datenschutz-Grundverordnung (DS-GVO) machen immer mehr Bürgerinnen und Bürger von ihrem Beschwerderecht Gebrauch. So haben mich 2020 mehr als doppelt so viele Beschwerden erreicht wie im Jahr 2018. Auch melden immer mehr verantwortliche Stellen Datenschutzverletzungen gemäß Artikel 33 DS-GVO.

Das thematische Spektrum von Beschwerden und gemeldeten Datenschutzverletzungen ist sehr breit. Dennoch lassen sich einige Schwerpunkte erkennen.

So beschwerten sich etwa Nutzer von Webseiten und sozialen Medien häufig über die Einbindung von (Tracking-)Diensten, die mangelhafte Verschlüsselung und unzureichende Transparenz auf Webseiten sowie vereinzelt über die Veröffentlichung von Fotos und Kommentaren in sozialen Medien.

Einen enormen Anstieg konnte ich bei den Beschwerden zur Videoüberwachung durch Privatpersonen verzeichnen. Sie verdoppelten sich 2020 im Vergleich zum Vorjahr. Allerdings stieg auch der Anteil der unbegründeten Beschwerden in diesem Bereich überproportional (siehe J.9.4, S. 183).

Eingaben aufgrund der Corona-Pandemie

Kontaktdaten zur Pandemiebekämpfung

Infolge der Corona-Pandemie mussten viele Unternehmen und Einrichtungen Daten von Kundinnen, Kunden und Teilnehmenden zur Kontaktnachverfolgung erheben (siehe J.1.1, S. 102). In diesem Zusammenhang erreichten mich zahlreiche Beschwerden über den nicht-datenschutzkonformen Umgang mit diesen Kontaktdaten, vor allem darüber, dass Kontaktlisten für jedermann frei zugänglich ausgelegt wurden. Ich habe den jeweiligen Unternehmen in diesen Fällen einen Hinweis über die datenschutzkonforme Führung der Kontaktlisten zukommen lassen.
Ebenfalls regelmäßigen Anlass zu Beschwerden gab die Datenübermittlung auf Vorrat von Kommunen an sonstige Stellen wie Polizeileitstellen oder Krankenhäuser ohne Rechtsgrundlage (siehe J.1.2 und J.1.9, S. 106 und 119). Auch zur unberechtigten Offenlegung von Daten gegenüber Dritten kam es im Zusammenhang mit der Corona-Pandemie, etwa dann wenn die Identität einer am Coronavirus erkrankten Beschäftigten allen weiteren im Unternehmen Tätigen bekannt gegeben wurde (siehe J.1.10, S. 121).

Personalausweiskopie ist möglich

Immer wieder erreichten mich auch Beschwerden von Bürgerinnen und Bürgern, von denen Unternehmen die Vorlage eines Personalausweises verlangten. Auffällig dabei war, dass die Beschwerdeführenden vielfach nicht wussten, dass das Kopieren und Scannen von Personalausweisen datenschutzrechtlich grundsätzlich nicht mehr zu beanstanden ist (siehe dazu meinen Tätigkeitsbericht 2017/18). Die Erhebung und Speicherung von Ausweiskopien sind jedoch an bestimmte Anforderungen geknüpft.

Gemäß § 20 Personalausweisgesetz darf der Personalausweis mit Zustimmung des Ausweisinhabers oder der Ausweisinhaberin abgelichtet werden. Die Ablichtung muss eindeutig und dauerhaft als Kopie erkennbar sein. Vom Ausweisinhaber bzw. der -inhaberin darf nicht verlangt werden, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Darüber hinaus muss die Datenverarbeitung entsprechend des Gebots der Datenminimierung nach Art. 5 Abs. 1 lit. c) DS-GVO auf das notwendige Maß beschränkt sein. Der Grundsatz der Speicherbegrenzung legt in Art. 5 Abs. 1 lit. e) DS-GVO fest, dass personenbezogene Daten in einer Form gespeichert werden sollen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie […] es erforderlich ist.

Werbung für Verstorbene

Betroffenenrechte werden nicht vererbt

Gelegentlich erreichten mich außerdem Beschwerden, in denen die Beschwerdeführenden vortrugen, Rechnungen oder Werbung erhalten zu haben, die an einen verstorbenen Verwandten adressiert waren. Die Hinterbliebenen hatten in diesen Fällen selten Verständnis dafür, dass die verantwortlichen Stellen die personenbezogenen Daten von Verstorbenen weiterhin für ihre Geschäftszwecke verwendeten. Vielfach wollten sie deshalb die Betroffenenrechte für die verstorbene Person geltend machen und die verantwortlichen Stellen um Löschung nach Art. 17 DS-GVO ersuchen oder Werbewiderspruch nach Art. 21 DS-GVO einlegen.

Die DS-GVO greift allerdings nicht für personenbezogene Daten verstorbener Personen. Mit dem Tode einer natürlichen Person gehen ihre Rechte nach der DS-GVO verloren und werden auch nicht an Hinterbliebene weitervererbt. Dadurch, dass die lebenden Verwandten auch nicht selbst von der Datenverarbeitung betroffen waren, konnten diese Eingaben auch nicht als Beschwerde im Sinne der DS-GVO behandelt werden.

Krimineller Datenhunger

Neben anderen Fällen der Infektion mit Ransomware und Viren sowie diversen Hacking-Angriffen erreichten mich vielfach Meldungen, in denen es in Unternehmen zu einem Befall mit der Schadsoftware „Emotet“ gekommen war. In diesen Fällen bat ich die Unternehmen zunächst, mir einen Abschlussbericht zur gemeldeten Datenschutzverletzung zukommen zu lassen. Daraus sollten insbesondere die ergriffenen technischen und organisatorischen Maßnahmen vor der Schutzverletzung sowie zur künftigen Vermeidung ähnlicher Verletzungen detailliert hervorgehen. Das macht es mir möglich, in einem zweiten Schritt die Geeignetheit und Angemessenheit des technisch-organisatorischen Datenschutzes zu bewerten. Zudem sollten aus dem Bericht die

Ursachen, die zur Schutzverletzung geführt haben, hervorgehen, so dass ich eine ausführliche Analyse der Schutzverletzung vornehmen kann.

Offene Verteilerlisten per E-Mail

Im Berichtszeitraum beschäftigte ich mich weiterhin mehrfach mit dem Problem offener Empfänger-Listen in E-Mail-Verteilern. Häufig wurden die Adressaten und Adressatinnen von Newslettern, Einladungen und Rundschreiben im CC-Feld des E-Mail-Programms eingetragen statt im BCC-Feld, wie es richtig gewesen wäre. Das hatte die Konsequenz, dass die Angeschriebenen sämtliche E-Mail-Adressen anderer Empfängerinnen und Empfänger übermittelt bekamen. Dieses Versäumnis steht auf der Rangliste der ständig wiederkehrenden Datenschutzfehler weit oben.

CC-Versand häufig durch Unachtsamkeit

Verantwortliche Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben nach Art. 24 Abs. 1 S. 1 DS-GVO die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften zu gewährleisten. Die verantwortliche Stelle muss daher alle zumutbaren Maßnahmen treffen, um derartige Offenlegungen von personenbezogenen Daten zu verhindern. Beim versehentlichen Versand per CC-Verteiler handelt es sich meist um menschliche Flüchtigkeitsfehler. Ich habe den betroffenen Stellen empfohlen, ihre Mitarbeitenden diesbezüglich regelmäßig zu schulen, um so datenschutzrechtliches Wissen präsent und aktuell für alle zu halten. Gleichzeitig könnten auch E-Mail-Programme implementiert werden, die von sich aus auf derartige Fehler hinweisen oder sie über entsprechende „Listenmanagement-Funktionen" bereits im Vorfeld ausschließen.

Versand von Unterlagen an Unberechtigte

Mehrfach gingen bei mir Beschwerden ein, in denen Betroffene nicht die für sie gedachten Schreiben, sondern die von anderen Personen per Briefpost erhielten. Die Empfängerinnen und Empfänger können die Schreiben öffnen und so unberechtigterweise Kenntnis von personenbezogenen Daten Dritter erlangen. Derartige Fehlübermittlungen gehen meist auf Unachtsamkeit zurück. Auch hier habe ich den betroffenen Stellen deshalb geraten, ihre Mitarbeitenden regelmäßig zu schulen.

Beschwerden zum Recht auf Auskunft

Vielen Unternehmen in Niedersachsen wissen, dass Betroffene ein unabdingbares und unentgeltliches Recht auf Auskunft nach Art. 15 DS-GVO über die zu ihrer Person gespeicherten Daten haben. Manchen Unternehmen scheint es aber nicht geläufig zu sein, dass sich die Reichweite des Auskunftsanspruches auch auf eine so genannte Negativauskunft erstreckt. Das heißt, Betroffene müssen auch eine Auskunft darüber erhalten, dass keine personenbezogenen Daten zu ihrer Person gespeichert sind.

Recht auf Negativauskunft

Ebenso erreichten mich immer wieder Beschwerden, in denen Bürgerinnen und Bürger unvollständige Auskünfte beklagten. Ich habe den Beschwerdeführenden in diesen Fällen empfohlen, zunächst von ihren Betroffenenrechten unmittelbar Gebrauch zu machen und die verantwortlichen Stellen mit der Bitte um Datenberichtigung nach Art. 16 DS-GVO zu ersuchen.

In vielen Fällen haben die Bürgerinnen und Bürger ihre Betroffenenrechte zudem gar nicht ausgeübt und baten mich darum, die verantwortlichen Stellen an ihrer statt um Auskunft nach Art. 15 DS-GVO zu ersuchen. Ich empfahl hier den Betroffenen, ihre Rechte zunächst selbst auszuüben. Wird die Auskunft dann nicht erteilt, werde ich in einem zweiten Schritt tätig.

Löschung von Kundendaten

Gesetzliche Fristen zur Aufbewahrung

Einige Bürgerinnen und Bürgern haben kein Verständnis dafür, dass ihre Kundendaten nicht sofort gelöscht werden (können), wenn sie eine Geschäftsbeziehung zu einem Unternehmen beenden. Nach Art. 17 Abs. 1 lit. a DS-GVO sind personenbezogene Daten zu löschen, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Soweit aber gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen, tritt an die Stelle einer Löschung nach Art. 17 Abs. 3 DS-GVO eine Sperre. Anstatt die personenbezogenen Daten zu löschen, kann die verantwortliche Stelle in diesen Fällen deren Verarbeitung einschränken.

Aufbewahrungsfristen ergeben sich für Kaufleute bereits aus § 257 Handelsgesetzbuch (HGB), wonach die einzelnen Geschäftsvorfälle in ihrer Entstehung und Abwicklung nachvollziehbar abzubilden sind, und für Steuerpflichtige auch aus § 147 Abgabenordnung (AO). Die Aufbewahrungsfrist beträgt gemäß § 257 Abs. 4 HGB für Buchungsbelege zehn Jahre und für Handelsbriefe sechs Jahre. § 147 Abs. 1 Nr. 2-4, Abs. 3 AO normiert die Aufbewahrungsfristen für die steuerlichen Belange. Handels- bzw. Geschäftsbriefe wie Eingangs- und Ausgangsrechnungen, Lieferscheine, Kostenvoranschläge und Verträge dürfen bereits von Gesetzes wegen innerhalb der maßgeblichen Frist von zehn Jahren nicht gelöscht werden.

Werbung trotz Werbewiderspruch

Für viele Betroffene stellt unverlangt zugestellte Werbung ein enormes Ärgernis dar. So gab es im Berichtszeitraum wieder zahlreiche Beschwerden über Unternehmen, die unaufgefordert Werbeschreiben und -E-Mails versandten und gelegentlich auf Auskunftsersuchen nach Art. 15 DS-GVO und Werbewidersprüche Betroffener nach Art. 21 DS-GVO nicht reagierten. Vielfach wurde in solchen Auskunftsersuchen nach Art. 15 DS-GVO auch die Frage gestellt, wie die zum großen Teil unbekannten Absender in den Besitz der (E-Mail-)Adressen gelangt sind und ob sie diese überhaupt für diese Zwecke nutzen durften.

Werbung bei Neukunden nur mit Einwilligung

E- Mail-Adressen, die unmittelbar von den betroffenen Personen im Rahmen einer Geschäftsbeziehung („Bestandskunden“) erhoben wurden, können grundsätzlich für E-Mail-Werbung genutzt werden. Allerdings muss dieser Zweck der E-Mail-Werbung entsprechend Art. 13 Abs. 1 lit c DS-GVO den betroffenen Personen bei der Datenerhebung transparent dargelegt worden sein. Falls bisher keine Geschäftsbeziehung mit dem Empfänger bestand („Neukundenwerbung“), ist die Verwendung von E-Mail-Adressen für Werbung nur dann erlaubt, wenn dafür vorher eine ausdrücklich erklärte Einwilligung abgegeben worden ist.

Die (E-Mail-)Adressen dürfen nur solange genutzt werden, bis die Betroffenen der Nutzung ihrer personenbezogenen Daten zum Zwecke der Werbung nach Art. 21 DS-GVO widersprechen. Einwilligungen in E-Mail-Werbung können allerdings auch erlöschen. Dies bezieht sich auf Fälle, in denen der Empfänger der E-Mail-Werbung vor langer Zeit eine Einwilligung abgegeben hat und

in der Zwischenzeit keine einzige Werbe-Mail von dem Verantwortlichen erhalten hat. Maßgeblich ist in diesem Fall, ob noch eine Erforderlichkeit zur weiteren Nutzung der Daten für Zwecke der Direktwerbung von dem Verantwortlichen nachvollziehbar dargelegt werden kann.

Betroffenenrechte wirklich ausüben

Des Öfteren erreichten mich schließlich Beschwerden darüber, dass Betroffene – wie von Unternehmen gefordert – ihre personenbezogenen Daten an diese übermitteln sollen. In vielen Fällen haben die Bürgerinnen und Bürger dabei ihre Betroffenenrechte nicht vollumfänglich ausgeübt.

Personenbezogene Daten dürfen nach Art. 6 DS-GVO nur verarbeitet werden, wenn eine der dort genannten Voraussetzungen vorliegt. Wurde keine Einwilligung erteilt und diente die Bearbeitung der personenbezogenen Daten weder der Erfüllung eines Vertrages noch einer rechtlichen Verpflichtung etc., kann es u.a. darauf ankommen, ob die Verarbeitung erforderlich war und ob Grundrechte und Grundfreiheiten der betroffenen Person das berechtigte Interesse des Verantwortlichen an einer Verarbeitung überwogen. Auch ohne eine Einwilligung kann die Verarbeitung personenbezogener Daten daher rechtskonform sein. Den Beschwerdeführenden empfahl ich, sich von den anfragenden Unternehmen eine Rechtsgrundlage für ihr Begehren nennen zu lassen. Denn nach meiner Beobachtung hat es sich bewährt, dass die Bürgerinnen und Bürger in vielen Fällen – soweit möglich – zunächst selbst ihre Betroffenenrechte ausüben, bevor ich tätig werde.

I.3. Das Recht auf Beschwerde bei der Aufsichtsbehörde

Jede betroffene Person hat das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde, wenn sie glaubt, dass eine bestimmte sie betreffende Datenverarbeitung gegen die Datenschutz-Grundverordnung (DS-GVO) verstößt. Beschwerden von Betroffenen sind zur Erfüllung meiner Aufgaben und zur Aufdeckung datenschutzwidriger Zustände unverzichtbar. In manchen Fällen hat die betroffene Person ganz konkrete Vorstellungen zur Bearbeitung ihrer Beschwerde durch die Aufsichtsbehörde, es bestehen jedoch nur eingeschränkte Rechte im Zusammenhang mit der Beschwerdebearbeitung.

Nach Art. 57 Abs. 1 Buchstabe f DS-GVO ist die Aufsichtsbehörde verpflichtet, sich mit einer Beschwerde zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und die Beschwerde führende Person innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Beschwerde zu unterrichten. Ansprüche auf eine bestimmte Form der Untersuchung, Entscheidung in der Sache oder aufsichtsbehördliche Maßnahmen gegenüber der Daten verarbeitenden Stelle bestehen dem gegenüber nicht.

Angemessene Prüfung der Beschwerde

Nicht in jedem Fall muss eine Beweisaufnahme durchgeführt werden

Die Beschwerde muss in angemessenem Umfang bearbeitet werden. Nach Erwägungsgrund 141 DS-GVO bestimmt sich die Angemessenheit nach dem Einzelfall. Dabei sind insbesondere die individuelle Bedeutung des Falles und die Schwere des möglichen Verstoßes zu berücksichtigen. Die Aufsichtsbehörde verfügt über ein Ermessen, wie und in welchem Umfang sie eine Beschwerde prüft und welche Maßnahmen sie gegebenenfalls gegen eine verantwortliche Stelle anordnet. Zum Beispiel ist es nach Betrachtung aller Umstände des Einzelfalles nicht in jedem Beschwerdefall sachgerecht, eine umfassende aufsichtsbehördliche Prüfung durchzuführen. Auch eine Entscheidung nach Aktenlage kann ausreichend sein, wenn die Sachlage eindeutig ist. Ebenso ist es oft nicht angebracht, eine umfangreiche Beweisaufnahme durchzuführen, wenn der Aufwand außer Verhältnis zur Schwere des vermeintlichen Verstoßes steht (so auch VG Hannover, Beschluss vom 01.04.20 - 10 A 3087/19). Bei jeder Bearbeitung einer Beschwerde muss meine Behörde auch auf die eigenen Möglichkeiten und Ressourcen Rücksicht nehmen (so auch VG Hannover, s.o.).

Rechtliche Bewertung der Beschwerde

Erhebt jemand Beschwerde wegen einer vermeintlich unzulässigen Datenverarbeitung, besteht manchmal bereits bei der betroffenen Person eine eigene rechtliche Einschätzung zum Beschwerdegegenstand und zur Auslegung der datenschutzrechtlichen Regelungen. Diese eigene Beurteilung hält allerdings in vielen Fällen einer rechtlichen Überprüfung durch die Aufsichtsbehörde nicht stand. Ebenso kann sich nach Prüfung der Beschwerde ergeben, dass der vorgeworfene Verstoß nicht festgestellt werden kann, wenn sich etwa der Sachverhalt anders darstellt als zunächst erwartet. Die rechtliche Beurteilung des Beschwerdegegenstandes liegt dabei ausschließlich in der Zuständigkeit der Aufsichtsbehörde.

Zuletzt entschied das OVG Koblenz (Urteil vom 26.10.20 – 10 A 10613/20.OVG), dass die rechtliche Würdigung der Aufsichtsbehörde auch nur einer eingeschränkten richterlichen Kontrolle unterliegt. Eine Klage gegen die ablehnende Entscheidung der Aufsichtsbehörde zu einer Beschwerde kann sich nur auf die ordnungsgemäße Entgegennahme, Prüfung und Bescheiderteilung beziehen, nicht auf das Ergebnis der Prüfung an sich. Eine betroffene Person hat immer die Möglichkeit, sich mit einer Klage direkt gegen die Daten verarbeitende Stelle zu wenden, um die streitigen Rechtsfragen zu klären. Das Beschwerdeverfahren ist hierfür nicht geeignet (so auch das OVG Koblenz, s.o.).

Klage kann sich nicht auf Ergebnis der Prüfung beziehen

Auswahl der aufsichtsbehördlichen Maßnahme

Ob und gegebenenfalls welche aufsichtsbehördliche Maßnahme gegen die verantwortliche Stelle ergriffen wird, liegt nach Art. 58 DS-GVO ebenfalls im Ermessen der Aufsichtsbehörde. Ein Anspruch von Beschwerdeführenden auf ein bestimmtes Tätigwerden der Aufsichtsbehörde besteht nicht (so auch VG Hannover, s.o.). Ein mit der Beschwerde geäußerter Wunsch bzw. Antrag ist hierbei nicht entscheidend. So wird manchmal bereits mit Einlegung der Beschwerde die Festsetzung eines Bußgeldes gegen die Daten verarbeitende Stelle beantragt. Die Entscheidung über eine Sanktionierung liegt allerdings allein im Ermessen der Aufsichtsbehörde, selbst bei einem eindeutig festgestellten Datenschutzverstoß. Die Frage der Sanktionierung hängt von vielen weiteren Aspekten des Falles ab, nicht zuletzt von der Schwere und Bedeutung des vorliegenden Falles im Vergleich zu anderen Verfahren.

Entscheidung über Sanktion liegt allein bei Aufsichtsbehörde

In manchen Fällen verlangen Beschwerdeführende, dass die Aufsichtsbehörde ihre personenbezogenen Daten bei der Daten verarbeitenden Stelle „sichert“ und für sie beschlagnahmt. Dies ist allerdings nicht Aufgabe der Aufsichtsbehörde und auch nicht vom Recht der Beschwerde umfasst. Das Beschwerderecht bietet keine Handhabe, eigene vermeintliche Ansprüche gegen die verantwortliche Stelle mit Hilfe der Aufsichtsbehörde durchzusetzen (so auch VGH Baden-Württemberg, Beschluss vom 22.01.20 - VGH 1 S 3001/19).

Die Entscheidung für eine konkrete repressive Maßnahme hängt von vielen Faktoren ab, welche allein die Aufsichtsbehörde in ihrer Gesamtheit bewerten kann. Eine Ausnahme besteht allerdings bei einer konkreten und unmittelbaren Gefahrensituation und einer Ermessensreduzierung auf null, etwa bei einem unkontrollierten, massenhaften Datenabfluss. Einzig in diesem Fall ist die Aufsichtsbehörde zum Einschreiten verpflichtet.

Umgang mit Beschwerden – Wahrung der Anonymität

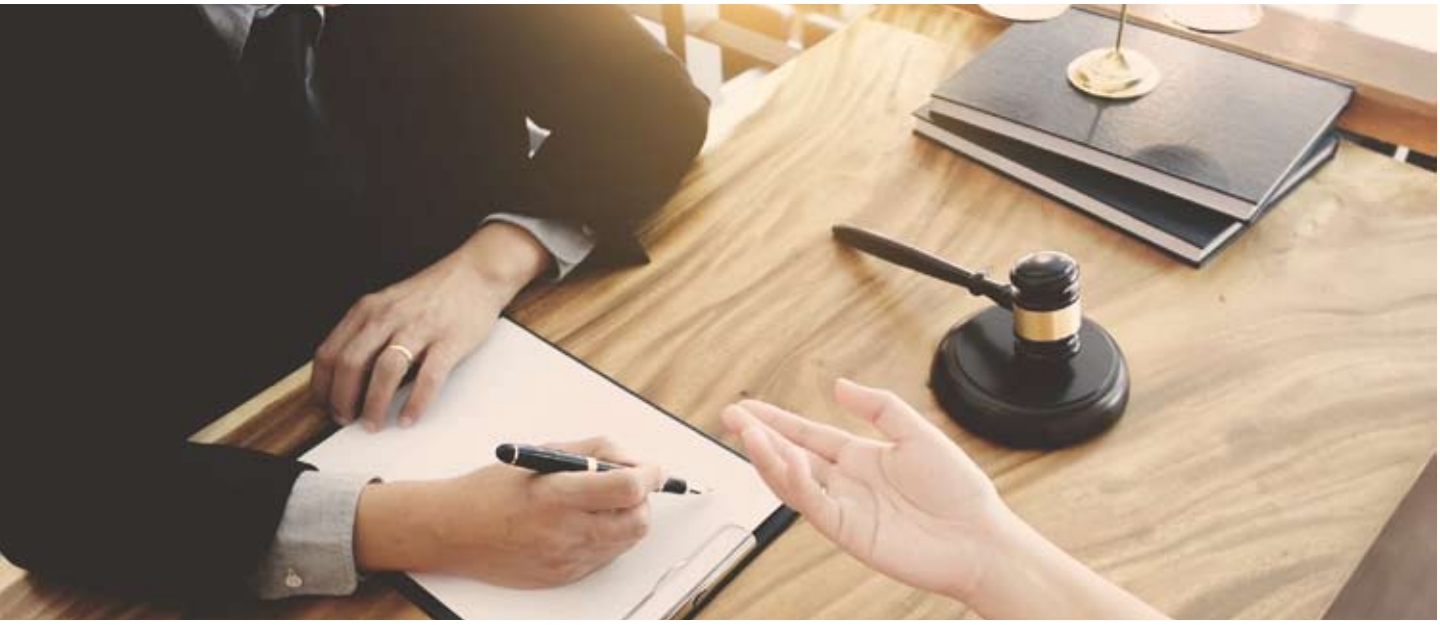
Als Aufsichtsbehörde prüfe ich jede Beschwerde sorgfältig. Bei manchen Beschwerden stellen meine Mitarbeiterinnen und Mitarbeiter jedoch fest, dass es sich im Ergebnis nicht um einen Datenschutzverstoß handelt. Jede Entscheidung über eine Beschwerde teile ich der Beschwerde führenden Person mit. Ebenso erläutere ich in den entsprechenden Fällen, warum ich keine Maßnahme gegen den Verantwortlichen getroffen habe.

Beschwerdeführende können sich grundsätzlich auf die Wahrung ihrer Anonymität verlassen. Meine Behörde gibt den Namen der Beschwerde führenden Person nicht weiter, wenn sie Verantwortliche zur Stellungnahme auffordert. Es sei denn, die Namensnennung ist erforderlich, um dem Verstoß nachgehen zu können, z. B. bei einer behaupteten Verletzung des Auskunftsrechts nach Art. 15 DS-GVO oder anderer Betroffenenrechte.

Informantinnen und Informanten müssen vor Nachteilen geschützt werden

Beantragen Verantwortliche Akteneinsicht bei mir, wird der Name der Beschwerde führenden Person in den Dokumenten unkenntlich gemacht. Dies ist insbesondere bei Beschwerden durch Beschäftigte gegen eine Datenverarbeitung durch die Arbeitgeberin oder den Arbeitgeber wichtig, um diese vor möglichen Nachteilen zu schützen. Dieses Vorgehen wurde durch ein Urteil des Verwaltungsgerichts Hannover vom 21. Januar 2020 (10 A 768/19) bestätigt. Nach Auffassung des Gerichts hat eine verantwortliche Stelle, die in einem von mir eingeleiteten Prüfverfahren den Namen der Beschwerde führenden Person ermitteln möchte, keinen Anspruch auf Akteneinsicht bezüglich des Schriftverkehrs zwischen der Aufsichtsbehörde und der Beschwerde führenden Person. Das Geheimhaltungsinteresse der Aufsichtsbehörde überwiegt hier aufgrund des überwiegenden öffentlichen Interesses am Schutz behördlicher Informantinnen und Informanten.

Allerdings kann die Anonymität des Beschwerdeführers bzw. der Beschwerdeführerin in einem aufgrund der Beschwerde eingeleiteten Ordnungswidrigkeitenverfahren nicht mehr gewährleistet werden. Im Ordnungswidrigkeitenverfahren besteht ein umfassendes Recht auf Akteneinsicht, eine Beschränkung wegen der Rechte Dritter ist anders als im Verwaltungsverfahren nicht vorgesehen.



I.4. Überblick über bearbeitete Bußgeldverfahren

Im Jahr 2020 hat die LfD Niedersachsen mit 10,4 Millionen Euro das bisher höchste Bußgeld unter Geltung der Datenschutz-Grundverordnung (DS-GVO) in einem Fall der Videoüberwachung ausgesprochen. Auch im Übrigen dominierten im Jahr 2020 verschiedene Konstellationen der Videoüberwachung. Zudem gab es Bußgeldverfahren betreffend GPS-Tracking, technisch-organisatorische Maßnahmen und zu Pflichten der Verantwortlichen.

Im Jahr 2020 habe ich insgesamt 82 neue Fälle unter Gesichtspunkten einer möglichen Geldbuße geprüft. Im gleichen Zeitraum habe ich 28 Bußgeldbescheide erlassen, die sich zum Teil auf Fälle bezogen haben, die bereits im Vorjahr eingeleitet worden waren. Von diesen Bescheiden sind 23 rechtskräftig geworden, da die Betroffenen entweder keinen Einspruch eingelegt haben oder weil sie ihre Einsprüche vor einer Sachentscheidung des Gerichts zurückgenommen haben. Die nicht mit Bußgeldern abgeschlossenen Verfahren sind entweder noch anhängig, waren nicht bußgeldwürdig, wurden eingestellt oder wurden an andere zuständige Stellen abgegeben.

Die LfD Niedersachsen hat im Jahr 2020 Bußgelder in Höhe von insgesamt 10,56 Millionen Euro festgesetzt. Die Bußgelder wurden gegen eine Rechtsanwaltsgesellschaft, ein Speditionsunternehmen, einen Arzneimittelhersteller, ein Industrieunternehmen sowie gegen natürliche Personen festgesetzt. Das höchste Bußgeld von gut 10,4 Millionen Euro richtete sich gegen die notebooksbilliger.de AG wegen unzulässiger Videoüberwachung im Betrieb betreffend Beschäftigte sowie Kundinnen und Kunden. Das Unternehmen hatte über mindestens zwei Jahre seine Beschäftigten per Video überwacht, ohne dass dafür eine Rechtsgrundlage vorlag. Das Bußgeld war bei Redaktionsschluss noch nicht rechtskräftig.

Pressemitteilung zu notebooksbilliger.de: https://t1p.de/pm-bussgeld

Geahndet wurden im Jahr 2020 Verstöße gegen die Artikel 5, 6, 13, 17, 31, 32 sowie 83 Absatz 5 lit. e DS-GVO und § 26 Bundesdatenschutzgesetz (BDSG) bzw. § 32 BDSG in der vor dem 25. Mai 2018 geltenden Fassung. Bei den Verstößen handelte es sich unter anderem um die Datenübermittlung an Dritte ohne Rechtsgrundlage, den unzulässigen Einsatz von Dashcams, die Nutzung veralteter Software mit Sicherheitslücken, die unzulässige Videoüberwachung, die Nichtbeachtung behördlicher Anweisungen und um die Missachtung auferlegter Auskunftspflichten.

Gerichtliche Entscheidungen

Im Jahr 2020 wurden durch die Gerichte fünf Entscheidungen zu Bußgeldverfahren getroffen, wobei sich die meisten auf Bußgeldbescheide des Vorjahres bezogen. In vier Verfahren wurde bestätigt, dass der Tatbestand verwirklicht war. Allerdings hatten die Betroffenen die Verstöße in der Sache auch überwiegend eingeräumt und ihre Einsprüche zumeist auf die Rechtsfolgenseite beschränkt. Bei solch einer Beschränkung wird die Feststellung des Verstoßes durch meine Behörde unmittelbar rechtskräftig, sodass das Gericht nur noch über die Höhe der Geldbuße zu entscheiden hat. Vier Einsprüche wurden vollständig zurückgenommen, bevor es zu einer gerichtlichen Entscheidung in der Sache kommen konnte. Zu einem Vorgang hat das Gericht weitere Ermittlungen für erforderlich gehalten.

Einzelne Fallkonstellationen

Videoüberwachung; Schwerpunkt Beschäftigtenkontext

Auffallend viele Fälle betreffen den Bereich der Videoüberwachung. Ein Schwerpunkt lag im Jahr 2020 erneut auf Verfahren, in denen Arbeitgeberinnen und Arbeitgeber ihre Beschäftigten per Video überwachen (siehe auch I.6, S. 90 und J.9.2, S. 179).[1] Dies geht in Extremfällen so weit, dass Beschäftigte bei jeder Bewegung von einer oder gar mehreren Kameras erfasst werden.

In einem Bußgeldverfahren verfolgt werden Fälle, in denen die Überwachung der Beschäftigten nicht im Einklang mit dem nach § 26 Bundesdatenschutzgesetz (BDSG) zu gewährleistenden Beschäftigtendatenschutz steht. Danach dürfen personenbezogene Daten von Beschäftigten nur aufgrund eng begrenzter Erlaubnistatbestände verarbeitet werden. Einerseits ist die Verarbeitung nach § 26 Absatz 1 Satz 1 BDSG zulässig, wenn sie zur Durchführung des Beschäftigungsverhältnisses erforderlich ist. Weiterhin wäre sie zulässig, wenn eine wirksame Einwilligung vorliegt, was aufgrund des Über-Unterordnungsverhältnisses im Beschäftigtenverhältnis und der zwingend notwendigen Freiwilligkeit der Einwilligung nur selten der Fall sein wird.[2]

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten gemäß § 26 Absatz 1 Satz 2 BDSG nur verarbeitet werden,

- wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat,
- die Verarbeitung zur Aufdeckung erforderlich ist
- und das schutzwürdige Interesse der oder des Beschäftigten am Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Datenerhebung nur bei konkretem Verdacht

Die Datenerhebung zu diesem Zweck erfolgt dann nur gegenüber jenen Beschäftigten, gegenüber denen ein konkreter Verdacht besteht. Die gesamte Belegschaft darf also nicht überwacht

1 Mein Vorgehen gegen Videoüberwachung am Arbeitsplatz habe ich bereits im vorangegangenen Tätigkeitsbericht des Jahres 2019 ausführlich dargestellt, siehe Seiten 173 ff.

2 Siehe Tätigkeitsbericht 2019, Seite 176.

werden. Hierzu bildete das Verwaltungsgericht Hannover in einem nicht veröffentlichten Urteil des Jahres 2020 folgenden Kernsatz heraus: „Die Beschäftigten müssen ihre Persönlichkeitsrechte nicht für einen Generalverdacht ihres Arbeitsgebers aufgeben."[3]

In Einzelfällen ist auch die Frage der Speicherdauer für eine Bußgeldentscheidung von Bedeutung, da die Eingriffsintensität mit der Speicherdauer ansteigt. Gemäß Artikel 17 Absatz 1 Buchstabe a DS-GVO müssen personenbezogene Daten – auch Videoaufzeichnungen – gelöscht werden, sobald sie zur Erreichung der Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Unter Berücksichtigung der Grundsätze der Datenminimierung und Speicherbegrenzung aus Artikel 5 Absatz 1 lit. c und e DS-GVO ergibt sich für Verantwortliche die Pflicht, Aufnahmen unverzüglich zu prüfen und gegebenenfalls zu löschen. Mit Blick auf die arbeitsfreie Zeit an den Wochenenden wird die Löschung daher in der Regel nach 72 Stunden zu erfolgen haben.

Allerdings sind Ausnahmen möglich, wenn die Löschung nach dieser Zeitspanne nicht für die Verfolgung legitimer Zwecke ausreicht. So können beispielsweise für externe Lagerstätten und Serverräume längere Speicherdauern hingenommen werden, wenn diese Bereiche fast nie betreten werden. Auch können längere Speicherdauern für Packarbeitsplätze im Logistikbereich hingenommen werden, sofern die Erfassung strikt auf den Tisch sowie die arbeitenden Hände beschränkt ist und mit der Überwachung keine Verhaltens- und/oder Leistungskontrolle verbunden wird.

Pflichtverstöße der Verantwortlichen

Verantwortliche müssen Transparenzpflichten nach Artikel 12 ff. DS-GVO sowie Mitwirkungs- und Meldepflichten aus Artikel 31 ff. DS-GVO erfüllen.

Verstöße gegen Artikel 13, 14 DS-GVO (Information der von der Verarbeitung betroffenen Personen) wurden von mir verfolgt, wenn mindestens ein weiterer Verstoß hinzukam, insbesondere ein Verstoß gegen Artikel 5, 6 DS-GVO. Singuläre Verstöße gegen Artikel 13, 14 DS-GVO wurden im Berichtszeitraum nicht verfolgt, wären künftig aber bei einer Vielzahl betroffener Personen oder bei besonders uneinsichtigen Verantwortlichen denkbar.

Auch Durchsuchungen sind möglich

Auch Verstöße gegen die Pflicht zur Zusammenarbeit nach Artikel 31 DS-GVO können zu Maßnahmen im Bußgeldverfahren führen. So ist etwa denkbar, dass bei unkooperativen Adressatinnen und Adressaten eine Durchsuchung durchgeführt wird (siehe I.6, S. 90). Weiterhin können unrichtige Angaben gegenüber der Aufsichtsbehörde im Verwaltungsverfahren zur Festsetzung einer Geldbuße führen, da auch damit gegen die Pflicht zur Zusammenarbeit verstoßen wird.

Verfolgt wird ebenfalls die Nichtbeachtung vollziehbarer behördlicher Anweisungen. Wenn sogar ausnahmsweise die sofortige Vollziehung der Anweisung gemäß § 80 Absatz 2 Satz 1 Nummer 4 Verwaltungsgerichtsordnung angeordnet wird, dient die Anweisung dazu, datenschutzrechtlich unerträgliche Zustände zu beseitigen. Setzen Verantwortliche sich über solche Anweisungen eigenmächtig hinweg und passen sie die Verarbeitung nicht an, sind neben den Zwangsmitteln des Verwaltungsverfahrens auch empfindliche Geldbußen geboten.

3 VG Hannover, Urteil vom 27. November 2020, 10 A 1882/19

GPS-Tracking

Polizei und Staatsanwaltschaften geben an meine Behörde Verfahren im Zusammenhang mit GPS-Trackern ab, die unerwartet an oder in Fahrzeugen gefunden wurden, wenn nicht zugleich eine Straftat vorliegt. Teilweise werden statt spezieller GPS-Tracker auch Mobiltelefone verwendet. Bei solch einem Fund ist anzunehmen, dass die Bewegungen des Fahrzeuges – und damit personenbezogene Daten der Fahrerinnen und Fahrer – von einer unbekannten dritten Person verfolgt wurden.

Meist lässt sich das gefundene Gerät über die eingelegte SIM-Karte einer bestimmten Person zuordnen. Mit den Merkmalen der Speicherkarte (Seriennummer) bzw. der Rufnummer ist eine Abfrage beim Telekommunikationsdienstleister möglich. Die Abfrage kann durch die Aufsichtsbehörden für den Datenschutz aufgrund § 113 Absatz 1 Satz 1, Absatz 3 Nummer 1 Telekommunikationsgesetz (TKG) erfolgen, da sie für die Verfolgung von Ordnungswidrigkeiten zuständig sind.[4]

Die Ordnungswidrigkeit besteht darin, dass für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich ist, die beim Einsatz von GPS-Trackern regelmäßig nicht vorliegt. In Betracht käme allenfalls Artikel 6 Absatz 1 Buchstabe f DS-GVO. Diese Vorschrift fordert eine Abwägung zwischen den Interessen derjenigen, die den Tracker einsetzen (Verantwortliche) und den Interessen der von der Verarbeitung betroffenen Personen. Verantwortliche werden in aller Regel keine Interessen an der heimlichen Überwachung mittels GPS-Trackern haben, die gewichtiger sein könnten als die Interessen der betroffenen Personen. Mangels Rechtmäßigkeit der Verarbeitung liegt in solchen Konstellationen ein Verstoß gegen Artikel 5 Absatz 1 Buchstabe a und Artikel 6 DS-GVO vor.

Bei der Festsetzung der Geldbußen gegenüber natürlichen Personen wegen GPS-Tracking habe ich das monatliche Nettoeinkommen der Bußgeldadressaten zugrunde gelegt. In Anlehnung an die Zumessung von Geldstrafen einerseits und an das Bußgeldkonzept der Datenschutzkonferenz für Unternehmen[5] andererseits, habe ich mindestens die Hälfte eines monatlichen Nettoeinkommens als Geldbuße festgesetzt. Die niedrigsten Festsetzungen ergaben sich für geständige Adressaten, die zuvor nicht in Erscheinung getreten sind. Bei meinen Festsetzungen habe ich darauf geachtet, dass ein Abstand zu den real drohenden Geldstrafen bei artverwandten Straftaten verbleibt. Allerdings ist es möglich, dass Geldbußen höher als Geldstrafen für ähnliche Taten ausfallen: Während die DS-GVO bei Verstößen im Sinne des Artikel 83 Absätze 5 und 6 Geldbußen bis 20 Mio. Euro vorsieht, können Geldstrafen bei Einzeltaten aufgrund § 40 Absatz 1 Satz 2, Absatz 2 Satz 3 Strafgesetzbuch maximal 10,8 Mio. Euro betragen.

4 Zu § 113 TKG erging eine Entscheidung des Bundesverfassungsgerichts (Beschluss vom 27.05.2020, 1 BvR 1873/13), wonach § 113 Absatz 1 Satz 1 TKG verfassungswidrig ist. Als problematisch wurde gesehen, dass es nicht einmal eines Anfangsverdachts für Abfragen bedurfte. Abfragende Behörden müssen nunmehr in jedem Fall einen Anfangsverdacht haben. Das TKG muss bis Ende des Jahres 2021 überarbeitet werden. Siehe dazu auch Entschließung der Datenschutzkonferenz vom 25.11.2020: „Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten"; abrufbar unter https://t1p.de/dsk-entschliessungen

5 Siehe zum Bußgeldkonzept der Datenschutzkonferenz ausführlich meinen Tätigkeitsbericht 2019, S. 100 ff.

Es kam im Jahr 2020 auch vor, dass ich Fälle des GPS-Tracking nicht als Ordnungswidrigkeit verfolgt habe, und zwar dann, wenn der sachliche Anwendungsbereich der DS-GVO nicht eröffnet war. So unterfällt die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten aufgrund Artikel 2 Absatz 2 Buchstabe c DS-GVO nicht den datenschutzrechtlichen Vorschriften. Der Gesetzgeber vermeidet mit dieser Regelung, dass jegliche Verarbeitung von Daten, so sie im engsten Kreis bleibt, unter die DS-GVO fällt. Die heimliche Verarbeitung von Standortdaten naher Familienangehöriger stellt zwar nicht notwendigerweise einen Verstoß dar, erscheint jedoch moralisch fragwürdig und kann im Einzelfall strafrechtlich relevant sein.

Dashcams

Zum Sonderkomplex der Dashcam-Geldbußen habe ich bereits im Tätigkeitsbericht 2019 ausführlich berichtet.[6] Auch im Jahr 2020 entfielen zahlreiche Bußgeldverfahren auf unzulässig eingesetzte Dashcams.

FAQ zu Dashcams: https://t1p.de/faq-dashcam

Die anhaltend hohe Zahl solcher Verfahren hatte ich zum Anlass genommen, die Rechtslage und die niedersächsische Praxis in einer FAQ umfassend aufzuarbeiten. Die Fragen und Antworten habe ich im Oktober 2020 veröffentlicht.

6 Siehe Tätigkeitsbericht 2019, S. 105 ff.

I.5. Bußgeldurteil des Landgerichts Bonn – erste Antworten auf wesentliche Fragen der Bußgeldpraxis

Seit Einführung der Datenschutz-Grundverordnung (DS-GVO) verhängen auch deutsche Aufsichtsbehörden Bußgelder in empfindlicher Höhe gegen Unternehmen. Mit dem Urteil des Landgerichts (LG) Bonn vom 11. November 2020[1] erging erstmals eine Entscheidung eines Gerichtes zu einem Bußgeld nach neuem Datenschutzrecht in Millionen-Höhe, welche sich mit wesentlichen Rechtsfragen der neuen Bußgeldpraxis befasst.

Wirksam, verhältnismäßig, abschreckend

Die DS-GVO sieht einen im Vergleich zu früherem Recht deutlich erhöhten Bußgeldrahmen von bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres vor. Bußgelder sollen nach Art. 83 Abs. 1 DS-GVO in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Folglich wurden auch in Deutschland bei Datenschutzverstößen gegen große Unternehmen hohe Bußgelder verhängt, z. B. rund 35 Millionen Euro gegen H&M durch die Datenschutzaufsichtsbehörde in Hamburg und 14,5 Millionen Euro gegen die Deutsche Wohnen SE durch die Berliner Aufsichtsbehörde. Dies steht im Einklang mit der Festsetzung hoher Bußgelder durch andere europäische Datenschutzaufsichtsbehörden.

Bußgeldkonzept der DSK: https://t1p.de/bussgeldkonzept

Zu einer Vereinheitlichung der Bußgeldpraxis innerhalb Deutschlands trägt das im Oktober 2019 veröffentlichte Bußgeldkonzept der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bei, welches eine einheitliche Zumessungsmethode vorsieht (siehe meinen Tätigkeitsbericht 2019, S. 100) und zu welchem sich das LG Bonn ebenfalls geäußert hat.

Der Fall: Authentifizierung im Call Center

Der vom LG Bonn entschiedene Fall behandelt einen datenschutzrechtlichen Verstoß beim Authentifizierungsverfahren im Call Center des Telekommunikationsdienstleisters 1&1 Telecom GmbH. Bei Anrufen im Call Center genügte

1 Az. 29 OWi 1/20

die Angabe des Namens und Geburtsdatums, um weitergehende Informationen zur angegebenen Person zu erhalten. In einem Fall führte dies zur Herausgabe der aktuellen Telefonnummer eines 1&1-Kunden an seine frühere Lebensgefährtin, welche die so erlangte Nummer zu belästigenden Anrufen nutzte. Der Betroffene beschwerte sich beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) als zuständige Aufsichtsbehörde über die ungenügende Sicherung seiner personenbezogenen Daten bei Anrufen im Call Center. Das Unternehmen 1&1 nahm den Vorfall zum Anlass, zunächst auf eine „Drei-Faktor-Authentifizierung" umzustellen und schließlich eine Authentifizierung per Service-PIN einzuführen.

Die Entscheidung der Aufsichtsbehörde

Der BfDI stellte einen Verstoß gegen die Pflicht zur Ergreifung angemessener technisch-organisatorischer Maßnahmen nach Art. 32 Abs. 2 DS-GVO fest und verhängte im Dezember 2019 ein Bußgeld in Höhe von 9,55 Millionen Euro gegen die 1&1 Telecom GmbH. Das zuvor eingesetzte Verfahren zur Authentifizierung genügte nach Ansicht der Datenschutzaufsichtsbehörde nicht den Anforderungen an einen sicheren Umgang mit den personenbezogenen Daten der Kundinnen und Kunden bei Anrufen im Call Center. Der Bußgeldbescheid wurde unter Verweis auf eine unmittelbare Verantwortlichkeit gegen das Unternehmen 1&1 selbst festgesetzt und enthielt folgerichtig keine Bestimmung einer konkret handelnden (Leitungs-)Person im Unternehmen. Die Berechnung des Bußgeldes erfolgte in Anlehnung an das DSK-Bußgeldkonzept und berücksichtigte dabei entscheidend den hohen Umsatz des Unternehmens.

Pressemitteilung des BfDI: https://t1p.de/pm-1-und-1

Verfahren und Entscheidung des LG Bonn

Im Ergebnis erklärte das LG Bonn die Festsetzung eines Bußgeldes in diesem Fall für dem Grunde nach gerechtfertigt, reduzierte allerdings das durch den BfDI festgesetzte Bußgeld in der Höhe deutlich auf 900.000 Euro. Dabei hatte das Gericht über wesentliche Rechtsfragen zur Festsetzung von Bußgeldern gegen Unternehmen zu entscheiden:

- Unter welchen Voraussetzungen ist die direkte Sanktionierung von Unternehmen zulässig, insbesondere wie verhält sich die Zurechnungsnorm des § 30 Abs. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) zu der unmittelbar angeordneten Haftung des Verantwortlichen in Art. 83 DS-GVO?
- Darf die Zumessung des Bußgeldes maßgeblich auf dem Umsatz eines Unternehmens beruhen? Und darf dabei der konzernweite Umsatz zugrunde gelegt werden?

Das LG Bonn entschied eindeutig zugunsten einer unmittelbaren Verbandshaftung des betroffenen Unternehmens, wonach die Verhängung eines Bußgeldes gegen ein Unternehmen nicht davon abhängt, dass der konkrete Verstoß durch eine Leitungsperson begangen wurde. Die Zurechnungsnorm des § 30 Abs. 1 OWiG sei im Datenschutzrecht nicht anwendbar. Art. 83 Abs. 4 bis 6 DS-GVO sehe eine Geltung des Funktionsträgerprinzips wie im europäischen Kartellrecht vor. Dies ergebe sich aus dem Verweis auf die entsprechenden Regelungen der Art. 101, 102 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) in Erwägungsgrund 150 und aus der Formulierung in Art. 83 DS-GVO, wonach Verantwortliche und Auftragsverarbeiter als Adressaten von Bußgeldern genannt seien. Datenschutzrechtlich Verantwortlicher sei das Unternehmen selbst. Die Anwendung von § 30 Abs. 1 OWiG würde gegenüber dem europäischen Haftungsmodell zu einer erheblichen Einschränkung der Bußgeldverhängung gegen Unternehmen

Gericht entscheidet zugunsten der Verbandshaftung

führen, wenn trotz Feststehens eines Datenschutzverstoßes die internen Verantwortlichkeiten aufzuklären wären. Eine Anwendung nationaler Zurechnungsvorschriften hätte eine vom europäischen Gesetzgeber nicht beabsichtigte unterschiedliche Sanktionierungspraxis zur Folge. Es genüge daher die Begehung eines Datenschutzverstoßes innerhalb des Unternehmens. Folgerichtig sei im Bußgeldbescheid auch keine Benennung einer bestimmten natürlichen Person erforderlich, welche die konkrete Tat begangen habe. Der Datenschutzverstoß selbst sei Gegenstand der Sanktionierung, nicht die dafür ursächliche Tat.

Es gilt der funktionale Unternehmensbegriff

Das Gericht entschied ebenso eindeutig, dass bei einer Berechnung eines Bußgeldes nach EU-Datenschutzrecht der europäische funktionelle Unternehmensbegriff gelte. Damit kommt es bei der Bestimmung des Bußgeldrahmens bei einem konzernangehörigen Unternehmen nicht auf den Umsatz des einzelnen Unternehmens an, sondern auf den gesamten konzernweiten Umsatz.

Letztlich reduzierte das LG Bonn das verhängte Bußgeld jedoch erheblich, weil es die festgesetzte Summe in diesem Einzelfall für unangemessen hoch ansah. Das Gericht kritisierte dabei auch die Anwendung der stark umsatzbezogenen Zumessungsmethode des DSK-Bußgeldkonzeptes. Eine Bemessung des Bußgeldes durch Ermittlung eines sich nach dem Umsatz richtenden Grundwerts für das Bußgeld, welches je nach Schwere des Datenschutzverstoßes mit einem Faktor multipliziert werde, möge nach Ansicht der Kammer bei Datenschutzverstößen von mittlerem Gewicht durchaus zu angemessenen Ergebnissen führen. Bei schweren Datenschutzverstößen umsatzschwacher Unternehmen und leichten Datenschutzverstößen umsatzstarker Unternehmen hätten allerdings die tatbezogenen Zumessungsgesichtspunkte in Art. 83 Abs. 2 S. 2 DS-GVO Vorrang. Im vorliegenden Fall sah das Gericht mildernde Umstände, welche das verhängte Bußgeld insgesamt trotz des hohen Umsatzes der 1&1 Telecom GmbH als nicht mehr verhältnismäßig erscheinen ließen. Es habe lediglich einen einzigen tatsächlichen Missbrauchsfall gegeben, das Unternehmen habe nicht vorsätzlich gegen das Datenschutzrecht verstoßen, es seien darüber hinaus keine sensiblen personenbezogenen Datum herausgegeben worden und das Unternehmen habe sich auch nach Aussage des BfDI sehr kooperativ gezeigt sowie das Authentifizierungsverfahren nach den Vorgaben der Aufsichtsbehörde geändert.

Auswirkungen auf die Bußgeldpraxis

Geldbußen werden gemäß Art. 83 Abs. 3 DS-GVO gegen den Verantwortlichen oder den Auftragsverarbeiter verhängt. Adressaten des Art. 83 DS-GVO sind somit sowohl natürliche als auch juristische Personen. Im Bereich des Datenschutzrechts sind damit Unternehmensgeldbußen ohne weiteres möglich. Bei Verstößen gegen Datenschutzregelungen in Unternehmen kommt es weiterhin nicht darauf an, ob eine Leitungsperson für den Verstoß verantwortlich ist oder ob irgendeine beschäftigte Person gehandelt hat.[2] Diese unmittelbare Haftung des Unternehmens als Verantwortlicher im Sinne des Datenschutzrechts stellt seit Inkrafttreten der DS-GVO die Auffassung der DSK dar und wurde nun durch das Urteil des LG Bonn ausdrücklich bestätigt und

2 Nach dem Berichtszeitraum hat das Landgericht Berlin mit Beschluss vom 28.01.2021 (526 OWi LG) 212 Js-OWi 1/20 entschieden, dass Bußgelder gegen juristische Personen nur verhängt werden könnten, wenn eine nachgewiesene konkrete Handlung von Leitungspersonen oder gesetzlichen Vertretern dargelegt werde, die zu dem Bußgeldtatbestand geführt habe. Die Staatsanwaltschaft hat hiergegen Beschwerde eingelegt.

bekräftigt. Die Unternehmen selbst sind von der DS-GVO angesprochene Adressaten der verschiedenen Pflichten, die sich aus dem Umgang mit personenbezogenen Daten ergeben. Auch ein Fehlverhalten einer einfachen beschäftigten Person erfolgt in diesem Verantwortungsbereich und rechnet die Haftung daher unmittelbar dem Unternehmen zu. Die Regelung des Art. 83 DS-GVO lässt keinen Raum für nationale Abweichungen in den einzelnen Mitgliedstaaten wie § 30 Abs. 1 OWiG im deutschen Recht. Die vorrangige Anwendung der DS-GVO ist daher folgerichtig. Die gerichtliche Bestätigung der Anwendung des Funktionsträgerprinzips trägt damit auch zu einer Vereinheitlichung der Sanktionspraxis gegenüber Unternehmen in der EU bei.

Damit bleibt auch für den häufig im Zusammenhang mit § 30 OWiG genannten § 130 OWiG kaum ein Anwendungsbereich. Geregelt ist darin ein eigener Tatbestand für Aufsichtspflichtverletzungen durch Inhaber, die dem Unternehmen zugerechnet werden können. Aufsichtspflichtverletzungen sind beim Funktionsträgerprinzip allerdings keine Voraussetzung der Ahndung, sodass es dieser speziellen Zurechnung nicht bedarf.

Die Einschätzung des Gerichts zur Schwere der Tat beruht im vorliegenden Fall darauf, dass die mangelhafte Ausgestaltung des Authentifizierungsverfahrens keine Gefahr der massenhaften Herausgabe von personenbezogenen Daten mit sensiblem Gehalt barg. Eine Reduzierung des Bußgeldes bei weniger schweren Verstößen wird in Niedersachsen auch bei umsatzstarken Unternehmen vorgenommen; insofern steht diese Praxis im Einklang mit den Vorgaben durch das LG Bonn. Der Umsatz bleibt dabei allerdings weiterhin ein wesentlicher Faktor für die Berechnung des Bußgeldes, damit Bußgelder auch bei großen Unternehmen noch abschreckende Wirkung entfalten können. Auch das DSK-Bußgeldkonzept sieht im Übrigen eine Anpassung der Bußgeldhöhe nach dem Schweregrad der Tat und nach sonstigen für oder gegen den Verantwortlichen sprechenden Umständen vor.

Umsatz bleibt wesentlicher Faktor der Berechnung

Wegen der Berücksichtigung der individuellen Ahndungsempfindlichkeit des jeweiligen Verantwortlichen wird der Umsatz bei der Festsetzung eines Bußgeldes immer eine Rolle spielen. Geldbußen in großer Höhe wird es also weiterhin geben. Angesichts der Entscheidung des LG Bonn ist künftig verstärkt darauf zu achten, dass die individuellen Gesamtumstände des Einzelfalles wesentlichen Einfluss auf die Bußgeldhöhe haben.

I.6. Durchsuchungen von Geschäfts- und Wohnräumen

Während die Durchsuchung und Beschlagnahme durch die Aufsichtsbehörde in der Vergangenheit eher die Ausnahme waren, gehören diese Maßnahmen inzwischen zu den typischen Ermittlungsmethoden im Bußgeldverfahren. Da dieses Vorgehen mit einigem Zeit- und Personalaufwand verbunden ist, betrachte ich es als letztes Mittel zur weiteren Aufklärung des Sachverhaltes.

Die erste Durchsuchung von Geschäftsräumen mit Beschlagnahme von Unterlagen durch meine Behörde fand im Jahr 2018 statt. 2020 kam es zu mehreren solcher Maßnahmen.

Abgrenzung zum Verwaltungsverfahren

Die Aufsichtsbehörden haben im Verwaltungsverfahren umfangreiche Ermittlungsbefugnisse. Diese sind ihnen mit Art. 58 Abs. 1 lit. b, e und f Datenschutz-Grundverordnung (DS-GVO) sowie § 40 Abs. 5 Bundesdatenschutzgesetz (BDSG) zugewiesen. Danach sind die Behörden befugt, Geschäftsräume zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten. Die Verantwortlichen müssen dies dulden. Sollten sich Verantwortliche weigern, kann sich die Aufsichtsbehörde bei Bedarf mit Hilfe der Polizei Zutritt zu den Geschäftsräumen verschaffen.

Keine Sicherstellung im Verwaltungsverfahren

Die Sicherstellung von Beweismaterial kommt im Verwaltungsverfahren allerdings nicht in Frage, da sie nach den polizeirechtlichen Vorschriften erfolgen müsste. Danach darf eine Sache nur sichergestellt werden, um eine gegenwärtige Gefahr abzuwehren.

Wenn eine weitere Aufklärung notwendig, das Verwaltungsverfahren dafür nicht geeignet und die Sache bußgeldwürdig ist, kann die weitere Aufklärung im Bußgeldverfahren erfolgen. Neben der Befragung von Zeuginnen und Zeugen sowie Sachverständigen kommen hier auch die Durchsuchung von Geschäfts- und Wohnräumen in Betracht. Das mit dem Strafverfahren verwandte Bußgeldverfahren kennt zudem die Sicherstellung von Sachen und Unterlagen als Beweismittel, nötigenfalls als Beschlagnahme gegen den Willen des Betroffenen.[1]

1 Anders als im Datenschutzrecht meint „Betroffener" im Sinne des Ordnungswidrigkeitenrechts die natürliche oder juristische Person, der eine Ordnungswidrigkeit vorgeworfen wird (§ 41 BDSG i.V.m. § 66 OWiG).

Abwägung zwischen Überprüfung und Durchsuchung

Eine Sachverhaltsaufklärung über das Bußgeldverfahren kommt in Betracht, wenn das schriftliche Verwaltungsverfahren keine hinreichende Aufklärung (mehr) verspricht und die Sache bußgeldwürdig erscheint. Dabei besteht die Auswahl zwischen zwei Maßnahmen vergleichbarer Eingriffstiefe: Zum einen die Durchführung eines Überprüfungsverfahrens im Rahmen eines unangekündigten Vor-Ort-Termins mit sofort vollziehbarem Verwaltungsakt der Behörde, wobei Verantwortliche zu dulden haben, dass die von der Behörde beauftragten Personen ihre Grundstücke und Geschäftsräume betreten und Zugang zu den Datenverarbeitungsanlagen und -geräten erhalten (§ 40 Absatz 5 Satz 2 BDSG). Zum anderen die Durchführung eines Bußgeldverfahrens mit unangekündigter Durchsuchung. Die Durchsuchung hat den Vorteil, dass ein Richter oder eine Richterin vorab die Argumente der Behörde überprüfen kann, was im Interesse der Betroffenen liegt.

Der Gesetzgeber hat für die Ordnungswidrigkeiten im Datenschutzrecht mit einem Regelbußgeldrahmen von bis zu 10 bzw. 20 Millionen Euro zum Ausdruck gebracht, welche erhebliche Bedeutung er dem Schutz personenbezogener Daten beimisst. Eine etwaige Beeinträchtigung der Betroffenen während der Nichtverfügbarkeit einzelner beschlagnahmter Sachen oder Unterlagen ist angesichts dieser Bedeutung hinzunehmen. Zudem kann die Beschlagnahme der Originalunterlagen und -datenträger in geeigneten Fällen durch Fotokopien bzw. Dateikopien ersetzt werden, um den Eingriff abzumildern.

Betroffene müssen Beschlagnahme hinnehmen

Verfahren und Ablauf

Die Befragung der Betroffenen sowie von Zeuginnen und Zeugen kann die Behörde selbst durchführen und sich bei unkooperativen Personen bei Bedarf der Polizei bedienen, wenn das Gericht die (zwangsweise) Vorführung von Betroffenen oder Zeuginnen und Zeugen anordnet[2]. Diese Rechte kommen ihr zu, da ihr die Befugnisse der Staatsanwaltschaft obliegen (§ 46 Absatz 2 OWiG).

Durchsuchungen stellen hingegen einen deutlich stärkeren Eingriff in die Rechte der Personen und Unternehmen dar. Nicht nur werden Räumlichkeiten betreten, es werden auch Unterlagen gesichtet und womöglich an einen anderen Ort gebracht. Mit dem Recht auf Unverletzlichkeit der Wohnung bzw. dem Recht am eingerichteten und ausgeübten Gewerbebetrieb sind zwei hohe Rechtsgüter betroffen. Durchsuchungen können daher gemäß § 105 Absatz 1 Satz 1 StPO i.V.m. § 46 Absatz 1 OWiG grundsätzlich nur durch einen Richter angeordnet werden. Ausnahmen sind bei Gefahr im Verzug möglich, also wenn der Verlust von Beweismitteln droht. In solchen Ausnahmefällen können meine Behörde bzw. die Polizei solche Anordnungen treffen.

Im Regelfall beantragt meine Behörde eine Durchsuchungs- und Beschlagnahmeanordnung bei Gericht. Der Antrag wird ausführlich begründet und beinhaltet Ausführungen zu den öffentlichen Interessen an der Verfolgung der Ordnungswidrigkeit und den gegenläufigen Interessen der Betroffenen im Einzelfall. Außerdem wird die Ermittlungsakte übersendet. Antrag und Akte

2 §§ 161a Absatz 1 Satz 1, 51 Absatz 1 Satz 3 Strafprozessordnung – StPO – in Verbindung mit § 46 Absätze 1 und 5 Satz 1 Gesetz über Ordnungswidrigkeiten – OWiG

geben dem Gericht die Möglichkeit, eine Abwägung vorzunehmen und über den Antrag zu entscheiden. Entscheidet das Gericht im Sinne der Behörde, erlässt es einen Beschluss und ordnet darin die Durchsuchung und Beschlagnahme an.

Organisation der Durchsuchung mit der Polizei

Anschließend wird die Durchsuchung zusammen mit den zuständigen Polizeidienststelle organisiert. Zu Beginn der Durchsuchung wird der Beschluss des Gerichts dem Adressaten oder der Adressatin eröffnet und ein Exemplar ausgehändigt. Die notwendigen rechtlichen Hinweise werden erteilt. Anschließend werden die Unterlagen oder Installationen (z.B. Videokameras) gesucht, die mit dem Vorwurf im Zusammenhang stehen. Wenn die Beweisrelevanz nicht ausgeschlossen werden kann, werden Unterlagen, Dateien, EDV-Datenträger – bis hin zu Servern – sichergestellt. Über sichergestellte Unterlagen und Gegenstände wird ein Sicherstellungsverzeichnis geführt, von dem der Adressat oder die Adressatin eine Ausfertigung erhält. Weiterhin wird die Durchsuchung protokolliert und etwaige Angaben von Betroffenen und anderer Personen darin aufgenommen. Denkbar sind auch begleitende Befragungen von Betroffenen und Zeuginnen und Zeugen.

Wenn Beschäftigte meiner Behörde teilnehmen, leiten sie – als Teil der Verfolgungsbehörde – die Durchsuchung. Auf die Hinzuziehung von Zeuginnen oder Zeugen kann dann verzichtet werden. Führt die Polizei die Durchsuchung alleine durch, wird regelmäßig ein Zeuge oder eine Zeugin der örtlichen Kommunalverwaltung hinzugezogen (§ 105 Absatz 2 StPO i.V.m. § 46 Absatz 1 OWiG).

Nach der Durchsuchung werden die sichergestellten Beweismittel ausgewertet, entweder durch die Polizei oder durch meine Behörde selbst (§ 110 Absatz 1 StPO i.V.m. § 46 Absatz 1 OWiG). Soweit elektronische Beweismittel Schwierigkeiten bereiten (ungewöhnliche Dateiformate, Verschlüsselung o.ä.), werden die Mitarbeiterinnen und Mitarbeiter meines IT-Labors hinzugezogen.

Sowohl vor, während als auch nach der Durchsuchung werden belastende sowie entlastende Umstände ermittelt. So kann es vorkommen, dass sich während der Durchsuchung oder später anhand der Beweismittel herausstellt, dass der Vorwurf nicht aufrechterhalten werden kann. Das Verfahren würde dann nach § 170 Absatz 2 StPO i.V.m. § 46 Absatz 1 OWiG aus tatsächlichen Gründen eingestellt.

Kooperation der Betroffenen

Betroffene müssen sich nicht äußern

Während der Durchsuchung kann die Behörde keine Kooperation der Betroffenen erwarten. Abgesehen von einigen Pflichtangaben (§ 111 OWiG) können sie schweigen. Sie müssen sich weder zum Vorwurf äußern noch müssen sie an der Durchsuchung mitwirken.

Wirken die Betroffenen mit, können sie die behördliche Maßnahme erheblich beschleunigen und womöglich den Eingriff abschwächen. Sind die gesuchten Unterlagen und Dateien gefunden und gesichert, wird die Maßnahme gewöhnlich beendet. Dann werden zumeist nur verhältnismäßig wenige Unterlagen und Gegenstände mitgenommen.

Ohne Mitwirkung ist es wahrscheinlicher, dass Computer oder sogar Server mitgenommen und zu einem späteren Zeitpunkt ausgewertet werden müssen. Dies kann einige Zeit in Anspruch nehmen. Entsprechend lange müssen Betroffene auf die sichergestellten Gegenstände verzichten.

Konkrete Fallkonstellationen 2020

Allgemeine Videoüberwachung

Bei zwei verschiedenen Unternehmen hatte ich die Videoüberwachung geprüft und beanstandet. Beide hatten nachgewiesen, die Videoüberwachung rechtmäßig umgestellt zu haben. Nach einiger Zeit gingen zu beiden Unternehmen glaubhafte Hinweise bei mir ein, dass die Überwachungsanlagen zumindest teilweise auf den ursprünglichen, rechtswidrigen Stand zurückgestellt worden seien.

Die Unternehmen hatten sich in der Zwischenzeit nicht an mich gewendet, um die Änderungen ihrer Anlage zu besprechen. Jedoch wussten sie aus den vergangenen Verfahren, wie sie eine Videoüberwachung rechtmäßig ausgestalten konnten. Eine erneute schriftliche Überprüfung erschien ungeeignet, da in diesem Fall der Verlust möglicher Beweismittel zu befürchten war.

In beiden Fällen habe ich vor Ort tatsächlich eine Videoüberwachungsanlage vorgefunden, die nicht dem Stand entsprach, der mir zuvor von den Unternehmen nachgewiesen worden war. Während ein Unternehmen die Videoüberwachung – auch soweit sie zulässig war – unmittelbar nach der Durchsuchung komplett abgebaut hat, wollte das andere Unternehmen die Videoüberwachung unverändert weiter betreiben. Beide Bußgeldverfahren sind noch nicht rechtskräftig abgeschlossen.

Keine Zusammenarbeit im Verwaltungsverfahren

Schreiben kommen ungeöffnet zurück

Verantwortliche sind nach Art. 31 DS-GVO verpflichtet, mit den Aufsichtsbehörden zusammenzuarbeiten. Dazu gehört insbesondere, dass Fragen der Behörden beantwortet werden. In einem Fall erreichte mich eine Beschwerde, dass öffentliche Flächen mit zahlreichen Kameras überwacht würden. Der mutmaßlich Verantwortliche reagierte weder auf Schreiben per einfacher Post noch auf zugestellte Auskunftsheranziehungsbescheide. Stattdessen ließ er förmlich zugestellte Schreiben kommentarlos an mich zurückgehen.

Da es keine sinnvolle weitere Möglichkeit der Aufklärung gab und ein Dauerverstoß im Raum stand, wurde eine Durchsuchung beantragt. Zwar wurden Kameras vorgefunden, die auch mit Strom versorgt wurden, um bei Dunkelheit ein Schimmern der Infrarotlampen zu erzeugen. An eine Aufzeichnungseinheit oder einen Bildschirm waren die Kameras indes nicht angeschlossen, sodass es sich funktional um Attrappen handelte.

Das Bußgeldverfahren wurde eingestellt. Jedoch musste der Verantwortliche die Belastung der Durchsuchung hinnehmen. Auch wenn Durchsuchungen möglichst unauffällig erfolgen, um Vorverurteilungen zu vermeiden, könnten Nachbarn eine Durchsuchung gerade bei beengten Platzverhältnissen wahrnehmen.

Wären die Fragen der Aufsichtsbehörde wahrheitsgemäß beantwortet und einen Nachweis über die funktionalen Attrappen vorgelegt worden, wäre dem Verantwortlichen diese Maßnahme erspart worden.

Dashcam

Ein Dashcam-Nutzer verwendete einen Ausschnitt seiner Aufzeichnungen, um mit einem Unternehmen eine außergerichtliche Lösung für ein aus Sicht des Dashcam-Nutzers strafbares Verhalten eines Fahrers des Unternehmens zu finden.[3] Das Unternehmen wendete sich daraufhin an mich.

Dashcam-Aufnahmen als Geschäftsmodell

Nach Prüfung des Sachverhaltes gelangte ich zu dem Schluss, dass neben der bekannten Aufzeichnung noch zahlreiche weitere existieren mussten. Außerdem bestand die Möglichkeit, dass der Betroffene bei weiteren Unternehmen außergerichtliche Lösungen anregte, wenn er der Auffassung war, auf seinen Dashcam-Aufnahmen sei entsprechendes Material zu finden.

Da im Auto des Betroffenen eine Dashcam vorgefunden wurde, wurde die Durchsuchung fortgesetzt und weitere Datenträger ausgewertet. Die sichergestellten Beweismittel gab die Polizei in Absprache mit mir bereits nach wenigen Tagen zurück, um den Eingriff für den Betroffenen so gering und kurzzeitig wie möglich zu halten. Durchgeführt wurde die Durchsuchung durch Einsatzkräfte der Polizei; erstmalig ohne Mitwirkung von Bediensteten meiner Behörde.

Die Durchsuchung wurde vom Landgericht als rechtmäßig bestätigt. Das Bußgeldverfahren ist allerdings noch nicht abgeschlossen.

3 Zur Dashcam-Nutzung siehe ausführlich meinen Tätigkeitsbericht 2019, S. 105 sowie die Zusammenstellung häufig gestellter Fragen, https://t1p.de/faq-dashcam.

I.7. Geldbußen wegen unzureichender technisch-organisatorischer Maßnahmen

Mit Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) können unzureichende technische und organisatorische Maßnahmen mit Geldbußen bis zu zehn Millionen Euro oder, sofern dieser Betrag höher ist, bis zu zwei Prozent des weltweiten Jahresumsatzes eines Unternehmens geahndet werden. Im Berichtszeitraum habe ich gegenüber dem Betreiber einer Internetseite einen Bußgeldbescheid über 65.500 Euro erlassen, weil die eingesetzte Software des Online-Shops veraltet war und erhebliche Sicherheitslücken enthielt.

Während vor Wirksamwerden der DS-GVO unzureichende technisch-organisatorische Maßnahmen (TOM) nicht unmittelbar bußgeldbewehrt waren, hat der Gesetzgeber in Artikel 25 DS-GVO und insbesondere in Art. 32 DS-GVO Anforderungen an TOM formuliert und Verstöße gegen die darin auferlegten Pflichten ausdrücklich von der Bußgeldvorschrift des Artikel 83 Absatz 4 Buchstabe a DS-GVO erfasst.

Was sind TOM?

Die DS-GVO fordert von Verantwortlichen und Auftragsverarbeitern, über TOM sicherzustellen, dass Risiken für personenbezogene Daten bereits vor der Verarbeitung geprüft, abgewogen und durch entsprechende Vorkehrungen minimiert werden. Diese Abwägung ist für jedes einzelne Verfahren notwendig. Zwar ist eine abschließende Auflistung nicht möglich, der Gesetzgeber nennt in Artikel 32 Absatz 1 DS-GVO jedoch typische Maßnahmen, die zu einem angemessenes Schutzniveau beitragen. Darüber hinaus verlangt Artikel 24 Absatz 1 Satz 2 DS-GVO, dass diese Maßnahmen nicht nur zum Zeitpunkt der Etablierung eines Verfahrens einen ausreichenden Schutz darstellen müssen, sondern auch zum Zeitpunkt der jeweiligen Verarbeitung. Der Verordnungsgeber verlangt dazu ausdrücklich, dass die „Maßnahmen [...] erforderlichenfalls überprüft und aktualisiert“ werden.

Risiken prüfen und minimieren

Pseudonymisierung und Verschlüsselung

Bei der **Pseudonymisierung** im Sinne des Artikels 4 Nummer 5 DS-GVO kann ein „Inhaltsdatensatz“ einer bestimmten Person nur mit Hilfe einer gesondert aufzubewahrenden Tabelle zugeordnet werden. Damit kann eine Pseudonymisierung bei Bedarf aufgehoben werden. Solche Verfahren kommen beispielsweise in der Forschung häufig zum Einsatz.

Ob und in welchem Umfang eine **Verschlüsselung** erforderlich ist, muss sich am Schutzbedarf und gegebenenfalls Besonderheiten der Verarbeitung ausrichten. Beim Versand von E-Mails mit sensiblem Inhalt kann beispielsweise eine Ende-zu-Ende-Verschlüsselung notwendig werden, wenn die Transportverschlüsselung nicht durchgängig gewährleistet werden kann und möglicherweise weitere Mailserver auf dem Transportweg verwendet werden. Die verwendeten Algorithmen haben sich dabei stets am Stand der Technik zu orientieren, sodass als nicht hinreichend sicher identifizierte Algorithmen nicht mehr zu verwenden sind.[1]

Sicherstellung der Gewährleistungsziele Vertraulichkeit, Integrität, Verfügbarkeit sowie Belastbarkeit der Systeme und Dienste

Das Standard-Datenschutzmodell sowie die ISO 27000-Normenreihe werden von diesen Gewährleistungszielen geleitet. Im Vordergrund steht der wirksame Schutz vor Zugriffen durch Unbefugte.

Rechte restriktiv vergeben

Grundsätzlich wird den Gewährleistungszielen hinreichend Rechnung getragen, wenn die Systeme ein dem im Zeitpunkt der Verarbeitung geltenden Stand der Technik vergleichbares Sicherheitsniveau bieten. Die **Vertraulichkeit** wird – neben der technischen Maßnahme der Verschlüsselung – mit organisatorischen Maßnahmen wie Zutritts-, Zugriffs-, Zugangs- und Weitergabekontrolle gewährleistet. Geeignete Maßnahmen zur Gewährleistung der **Integrität** sind eine restriktive Rechtevergabe nach dem Grundsatz, dass alles verboten ist, was nicht ausdrücklich erlaubt ist. Darüber hinaus können Maßnahmen wie Signierung der Daten, Prüfsummen und Protokollierung dabei unterstützen, Verletzungen der Datenintegrität zu erkennen. Daneben sind Maßnahmen zur Gewährleistung der Integrität der Systeme im Sinne der IT-Sicherheit (wie Untersuchung auf Schwachstellen, Netztrennungen und Penetrationstests) geeignet, die Gefahr einer datenschutzrechtlichen Integritätsverletzung zu minimieren.

Die **Verfügbarkeit** wird durch Maßnahmen wie redundante Auslegung der Systeme, zusätzliche Absicherung der Stromversorgung und mehrstufige Datensicherungen erreicht. Bei Systemen, die aus dem Internet oder anderen unsicheren Netzen erreichbar sind, kommen der Schutz vor Überlastangriffen neben gewöhnlichen Firewall-Systemen zum Einsatz. Mit **Belastbarkeit** ist eine Widerstandsfähigkeit gegen unvorhergesehene Störungen gemeint, was unter anderem die Reduzierung von Angriffsflächen sowie Maßnahmen zum Schutz vor gezielten Überlastungen umfasst.

Die ergriffenen Maßnahmen müssen jederzeit wirksam sein und sind daher in regelmäßigen Abständen zu überprüfen.

Fähigkeit, die Verfügbarkeit und den Zugang zu personenbezogenen Daten bei einem Zwischenfall rasch wiederherzustellen

Tritt trotz der gerade beschriebenen Vorsorge ein Krisenfall ein, müssen Verantwortliche in der Lage sein, die personenbezogenen Daten in angemessener Zeit wiederherstellen und darauf zugreifen zu können. Artikel 32 Absatz 1 Buchstabe c DS-GVO fordert zur Gewährleistung der Sicherheit der Verarbeitung die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Notfall- und Krisenkonzept erstellen

Um im Krisenfall den Geschäftsbetrieb aufrecht erhalten zu können, benötigen Verantwortliche ein Notfall- und Krisenkonzept. Dieses kann beispielsweise eine Notstromversorgung, Vertre-

1 Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen": https://t1p.de/bsi-krypto

tungspläne für das IT-Personal und ein betriebliches Kontinuitätsmanagement beinhalten.
Zudem sollte die Funktionsfähigkeit des Konzeptes überprüft werden. So soll die vollständige Wiederherstellungsfähigkeit der erstellten Backups auf geeigneten Testsystemen regelmäßig geprüft werden.

Regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit

Die technische Entwicklung macht es notwendig, die ergriffenen Maßnahmen regelmäßig auf ihre Wirksamkeit zu überprüfen. Beispielsweise können sich verwendete Verschlüsselungsverfahren durch neu entdeckte Schwachstellen sowohl im Hinblick auf den verwendeten Algorithmus, als auch auf dessen konkrete Implementierung oder durch gesteigerte Rechenleistung als unsicher erweisen.

Regelmäßige Trainings von Beschäftigten

Zur Überprüfung der Maßnahmen kann eine Vielzahl von Methoden eingesetzt werden. So könnten mit Penetrationstests Angriffsvektoren identifiziert werden, die bei integrierten Schwachstellenscans bzw. Build-in-Self-Tests der verwendeten Hard- und Software möglicherweise nicht auffallen. Hinsichtlich organisatorischer Maßnahmen kommen vor allem Evaluierungen durch Verantwortliche sowie regelmäßige Trainings von Beschäftigten in Betracht.

Weiter ist auch die Wirksamkeit von Maßnahmen zum Schutz vor betrügerischen Angriffsversuchen gegenüber Beschäftigen regelmäßig zu überprüfen. Zu diesen Versuchen zählt das Social Engineering, dessen Ziel es ist, durch zwischenmenschliche Beeinflussung vertrauliche Informationen insbesondere von Beschäftigten zu erlangen. Mit einigen Rahmeninformationen können Beschäftigte eines Unternehmens in ein Gespräch verwickelt werden, in dem sich Anrufer beispielsweise als Techniker oder Technikerin ausgeben, die noch Zugangsdaten benötigen. Unternehmen sollten ihre Beschäftigten im Rahmen ihrer Informations- und Hinweispflichten darauf hinweisen, dass es Penetrationstest und auch simulierte Social-Engineering-Angriffe geben kann, in deren Rahmen möglicherweise auch Beschäftigtendaten verarbeitet werden.

Bußgeld wegen des Betriebs einer Internetseite mit veralteter Software

Ich nahm eine Meldung gem. Artikel 33 DS-GVO zum Anlass, die Internetseite eines Unternehmens unter technischen Gesichtspunkten zu prüfen. Dabei stellte sich heraus, dass auf der Seite die Web-Shop-Anwendung xt:Commerce in der Version 3.0.4 SP2.1 verwendet wurde. Diese Version ist seit spätestens 2014 veraltet und wird vom Hersteller nicht mehr mit Sicherheitsupdates versorgt. Die genutzte Software enthielt erhebliche Sicherheitslücken, auf welche der Hersteller hingewiesen hatte. Die Sicherheitslücken ermöglichten unter anderem SQL-Injection-Angriffe. Auch der Hersteller warnte davor, die Version 3 der Software weiter einzusetzen.

Mit SQL-Injection-Angriffen können Angreifer in den Besitz der Zugangsdaten aller in der Anwendung registrierten Personen kommen. Dieser Angriffsvektor entsteht, wenn nicht alle vom Endanwender veränderbare Eingaben so maskiert werden, dass die Datenbank sie nicht als Befehl verstehen kann. Ohne Maskierung führt die Datenbank jeglichen Befehl mit eigenen Rechten aus. So können ganze Datenbanktabellen ausgegeben oder gelöscht werden. Auch das Herunterfahren des Servers kann möglich sein.

Berechnung der Passwörter war möglich

Meine Ermittlungen ergaben, dass die in der Datenbank abgelegten Passwörter zwar mit der kryptographischen Hashfunktion „MD5" gesichert waren, welche allerdings nicht auf den Einsatz für Passwörter ausgelegt ist. Eine schnelle ‚Berechnung' der Klartext-Passwörter wäre daher möglich gewesen. Auch existieren sog. „Rainbow-Tables" im Internet, anhand derer – ganz ohne Berechnung – das zu einem Hash gehörige Passwort abgelesen werden kann.

Hinzu kam, dass kein „Salt" verwendet wurde. Ein solcher Salt, der für jedes Passwort individuell generiert wird, verlängert ein Passwort und erschwert so die systematische Berechnung deutlich. Ziel des Salt ist es, dass der Angreifer für jedes Passwort eine komplette Neuberechnung durchführen muss und vorgefertigte Rainbow-Tables wertlos werden. Ohne Salt genügte hingegen eine gemeinsame Berechnung für die komplette heruntergeladene Datenbank.

Ohne entsprechende Sicherheitsvorkehrungen wäre es im vorliegenden Fall mit überschaubarem Aufwand möglich gewesen, die Klartext-Passwörter zu ermitteln und dann weitere Angriffsvektoren auszuprobieren. Ein Angreifer hätte die ermittelten Passwörter z.B. bei den ebenfalls in der Datenbank hinterlegten E-Mail-Adressen testen und im Erfolgsfall erhebliche (Folge-)Schäden anrichten können.

Häufig genügt aktuelle Software, um Sicherheitslücken zu schließen

Die Implementierung einer Salt-Funktion sowie eines aktuellen, auf Passwörter ausgelegten Hash-Algorithmus, wäre für das Unternehmen nicht mit unverhältnismäßigem Aufwand verbunden gewesen, vor allem, wenn diese Funktionalität mit neueren Versionen der Software eingepflegt wird. Dies gilt ebenso für die Beseitigung bekannter Sicherheitslücken, für die Aktualisierungen bereitstehen. Regelmäßig genügt also bereits die Aktualisierung der Software, um bekannt gewordene Sicherheitslücken und weitere Schwachstellen zu schließen. Dies kann mit Beschaffungs- und Umsetzungskosten verbunden sein, die jedoch grundsätzlich keinen unverhältnismäßigen Aufwand darstellen.

Die von der Verantwortlichen ergriffenen technischen Maßnahmen waren damit nicht dem Schutzbedarf gemäß Art. 25 DS-GVO angemessen, sodass ich einen Verstoß gegen Artikel 32 Absatz 1 DS-GVO festgestellt habe. Ich habe eine Geldbuße in Höhe von 65.500 Euro festgesetzt, die das Unternehmen akzeptiert hat.

Bei der Zumessung der Geldbuße konnte ich berücksichtigen, dass das Unternehmen bereits vor dem Bußgeldverfahren die betroffenen Personen darüber informiert hatte, dass ein Wechsel des Passwortes notwendig ist.

Absicherung von Passwörtern

Empfehlungen des BSI: https://t1p.de/bsi-krypto

Die Anforderungen an Passwörter sind aus Sicht des Datenschutzes und der Informationssicherheit identisch. Stets aktuelle Empfehlungen gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seiner Internetseite sowie in der technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" (BSI TR-02102-1). Da sich die Empfehlungen aufgrund neuerer Erkenntnisse ändern können, bietet dieser Beitrag lediglich eine Momentaufnahme.

Statt einer bei der Berechnung sehr effizienten Funktion wie MD5 sollte eine speziell für Passwörter entwickelte kryptographische Hashfunktion verwendet werden. Um Passwörter durch systematisches Ausprobieren (Brute-Force-Methode) zu ermitteln, bedarf es bei speziell für Passwörter vorgesehenen Funktionen[2] deutlich mehr Rechenaufwand. Weiterhin sollte für jedes Passwort ein individueller Salt gebildet werden. Das führt dazu, dass soviel Rechenleistung investiert werden muss, dass es uninteressant werden kann, die Passwörter der gesamten Datenbank zu ermitteln.

Handlungsempfehlung sichere Authentifizierung: https://t1p.de/sichere-auth

Allerdings kann es einzelne Zugänge geben, die für Angreifer besonders von Interesse sind. Das können vor allem Administrationszugänge und Zugänge prominenter Personen sein. Die Schwachstelle bleibt daher das vom Nutzer oder der Nutzerin gewählte Passwort. Dabei gilt, dass die Passwortstärke von seiner Länge deutlich stärker beeinflusst wird als von der Komplexität (Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen). Jedoch können auch längere Passwörter mit überschaubarem Aufwand ermittelt werden, wenn sie sich in Kennwortlisten finden. Die Nutzerinnen und Nutzer sollten daher keine Sprichwörter oder Zitate als Passwörter verwenden.

Feste Regeln für die Länge und Komplexität für Passwörter gibt es nicht. Wann ein Passwort ausreichend stark ist, hängt auch von der Umgebung und den typischen Angriffsvektoren ab. Wird der Zugang beispielsweise nach drei bis fünf Fehleingaben für einen längeren Zeitraum gesperrt oder ein zusätzliches Medium nach Fehlversuchen einbehalten (z.B. EC-Karte), genügt ein kürzeres und weniger komplexes Passwort.

Bei hohen Risiken oder sensiblen Daten sollte zudem eine Mehr-Faktor-Authentifizierung zum Einsatz kommen. Neben Benutzerkennung und persönlichem Passwort könnten beispielsweise Einmal-Passwörter versendet oder Security-Token eingesetzt werden.

Weitere Bußgeldverfahren mit Bezug zu technisch-organisatorischen Maßnahmen

Auch in anderen Verfahren spielen Verstöße gegen Artikel 25 und 32 DS-GVO eine Rolle, wenn auch häufig untergeordnet. So können Videoaufnahmen mangels Rechtsgrundlage gegen Artikel 6 DS-GVO oder § 26 BDSG verstoßen, Zugleich kann auch ein Verstoß gegen Artikel 25 DS-GVO vorliegen, wenn die Bereiche, in denen sich Personen bewegen oder aufhalten, nicht verpixelt wurden. Entgegen Art. 25 Absatz 2 DS-GVO hat der Verantwortliche in solchen Fällen keine geeigneten technischen Maßnahmen durch Voreinstellung getroffen, dass nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Vorrang hat in solch einem Fall der Verstoß gegen Artikel 6 DS-GVO bzw. § 26 BDSG.

2 Als geeignete Funktion nennt das BSI in der technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" (Stand März 2020, a.a.O.) einzig „Argon2id".

I.8. Die Verwarnung als verbindliche Feststellung eines Verstoßes

Die Datenschutz-Grundverordnung (DS-GVO) gewährt den Aufsichtsbehörden verschiedene Abhilfebefugnisse, eine davon ist die Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO. Die datenschutzrechtliche Verwarnung zeichnet sich durch die Feststellung eines bereits beendeten Verstoßes aus, der mit einer Rüge durch die Aufsichtsbehörde verbunden ist.

Die Vielzahl verschiedener Abhilfebefugnisse in der DS-GVO soll vor allem zu einer gleichwertigen aufsichtsbehördlichen Tätigkeit in den Mitgliedstaaten der EU beitragen. Die Auswahl der angemessenen Maßnahme steht dabei im Ermessen der Aufsichtsbehörde. Der Verwarnung kommt eine besondere Bedeutung zu, da es sich um die formelle Feststellung eines konkreten datenschutzrechtlichen Fehlverhaltens handelt und sie daher in vielen Fällen das passende Mittel als Reaktion auf einen Verstoß darstellt.

Feststellung eines Verstoßes

Förmlicher Tadel der Aufsichtsbehörde

Die Verwarnung ist zunächst ein deutlicher Hinweis an den Adressaten oder die Adressatin, dass die durchgeführte Datenverarbeitung rechtswidrig war. Anders als die Warnung nach Art. 58 Abs. 2 lit. a DS-GVO, die einen hypothetischen, noch nicht eingetretenen Sachverhalt behandelt, ist die Verwarnung die Reaktion auf einen bereits begangenen Datenschutzverstoß. Mit der Verwarnung hat die Aufsichtsbehörde die Möglichkeit auf einen rechtswidrigen Zustand zu reagieren, bei dem eine Anordnung nicht mehr vorgenommen werden kann, da der Verarbeitungsvorgang bereits von der verantwortlichen Stelle selbst beendet wurde oder sich erledigt hat.
Die Verwarnung ist jedoch mehr als die förmliche Feststellung eines Verstoßes. Gleichzeitig spricht die Aufsichtsbehörde einen förmlichen Tadel aus. Damit ähnelt die Verwarnung der früheren förmlichen Beanstandung, welche die Aufsichtsbehörden gegen öffentliche Stellen aussprechen konnten, um eine rechtswidrige Verarbeitung festzustellen und zu rügen.

Wirkung der Verwarnung

Die Verwarnung ist mehr als ein informeller Hinweis an Verantwortliche zu einer durchgeführten Datenverarbeitung. Denn die Aufsichtsbehörde nutzt dieses Instrument nur, wenn sie die in Rede stehende Datenverarbeitung bereits geprüft und einen Verstoß festgestellt hat. Die Verwarnung stellt damit eine formelle Ahndung eines Verstoßes dar. Zwar verfügt sie als reine Feststellung über keinen vollstreckbaren Inhalt. Dennoch sollten die Wirkungen

einer Verwarnung im Einzelfall nicht unterschätzt werden: Als Folge besteht ein aktenkundiges Fehlverhalten von Verantwortlichen, welches gegebenenfalls bei einem späteren Ordnungswidrigkeitenverfahren strafschärfende Wirkung haben dürfte, soweit ein Wiederholungsfall angenommen werden kann.

Die Verwarnung als Verwaltungsakt

Die Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO ist als feststellender Verwaltungsakt im Sinne des Niedersächsischen Verwaltungsverfahrensgesetzes anzusehen. Hierfür sprechen mehrere Argumente:

Verwarnung bildet Abschluss des Verwaltungsverfahrens

- Wie oben dargestellt, handelt es sich bei der Verwarnung eben nicht lediglich um einen Hinweis ohne weitere Wirkung für die Verantwortlichen. Die Aufsichtsbehörde hat hier zuvor den konkreten Sachverhalt geprüft und abschließend rechtlich bewertet.
- Die Verwarnung reiht sich zudem ein in die in Art. 58 Abs. 2 DS-GVO aufgezählten förmlichen Abhilfemaßnahmen.
- Ebenso erfolgt mit der Verwarnung der förmliche Abschluss des Verwaltungsverfahrens.
- Zwar werden den Verantwortlichen bei der datenschutzrechtlichen Verwarnung keine unmittelbaren Rechtspflichten auferlegt. Allerdings erfolgt eine rechtsverbindliche Feststellung der Aufsichtsbehörde bezüglich der rechtlichen Beurteilung der jeweiligen Datenverarbeitung. Dies hat Regelungswirkung für die Verantwortlichen.

Das Instrument der Verwarnung nutze ich immer dann, wenn einer verantwortlichen Stelle ihr rechtswidriges Handeln deutlich gemacht werden soll, gegebenenfalls auch in Kombination mit einem nachfolgenden Bußgeldverfahren. Bagatellfälle, z. B. bei einer nur unwesentlich verspäteten Auskunftserteilung oder einem nur geringfügig unvollständigen Verzeichnis der Verarbeitungstätigkeiten, bleiben außer Betracht. Allen datenschutzrechtlich Verantwortlichen ist zu raten, Verwarnungen der Aufsichtsbehörde ernst zu nehmen und das künftige Verhalten entsprechend anzupassen.

J. Aktuelle Themen

J.1. Datenschutz und Corona

1.1 Erfassung von Kundendaten mit Kontaktlisten

Ab Mai 2020 waren Gewerbebetriebe und Bildungseinrichtungen durch die Niedersächsische Corona-Verordnung (Corona-VO) verpflichtet, die Kontaktdaten von Kundinnen und Kunden bzw. Teilnehmenden zu erfassen. Im Fall einer Infektion mit dem Corona-Virus sollte damit die Nachverfolgung von Infektionsketten gewährleistet werden. Zahlreiche Beschwerden haben gezeigt, dass der datenschutzkonforme Umgang mit den erhobenen Daten vielfach Probleme bereitete oder ignoriert wurde.

Durch die Corona-VO wurden Betriebe und Einrichtungen mit Publikumsverkehr verpflichtet, Listen zu führen, in denen alle Kundinnen und Kunden bzw. Teilnehmenden mit Namen, Adresse und Telefonnummer erfasst wurden. So sollte das zuständige Gesundheitsamt im Falle eines Kontaktes mit einer Corona-infizierten Person in die Lage versetzt werden, Kontaktpersonen informieren zu können.

Rechtsgrundlage für die Datenerhebung

Für jede Verarbeitung personenbezogener Daten, so auch für die Listen zur Kontaktverfolgung, ist eine rechtliche Grundlage nach Art. 6 Datenschutz-Grundverordnung (DS-GVO) erforderlich, auf die Verantwortliche den jeweiligen Verarbeitungsvorgang stützen können müssen.

Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung

Auf die in der Corona-VO beschriebene Verarbeitung von Kontaktdaten findet Art. 6 Abs. 1 lit. c DS-GVO Anwendung. Nach dieser Vorschrift ist eine Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der die Verantwortlichen unterliegen. Eine solche rechtliche Verpflichtung für die Erfassung von Namen, Vornamen und Kontaktdaten der Kundinnen und Kunden bzw. Teilnehmenden ergibt sich aus den jeweils für unterschiedliche Verantwortliche geltenden Regelungen der Corona-VO.

Zweifel im Saarland

Der Saarländische Verfassungsgerichtshof entschied am 28. August 2020, dass die in der Saarländischen Corona-Verordnung geregelte Kontaktdatenerhebung verfassungswidrig ist, da es an einer parlamentsgesetzlichen Rechtsgrundlage fehlt.[1] Da die Rechtslage in Niedersachsen vergleichbar ist, bat ich das Niedersächsische Sozialministerium und die Niedersächsische Staatskanzlei, zeitnah eine gesetzliche Regelung für die Kontaktdatenerhebung zu schaffen. Dabei verwies ich auf die ständige Rechtsprechung des Bundesverfassungsgerichts, wonach Einschränkungen des Rechts auf informationelle Selbstbestimmung einer gesetzlichen Rechtsgrundlage bedürfen, die dem Gebot der Normenklarheit und dem Grundsatz der Verhältnismäßigkeit entsprechen muss.[2]

Exekutives Recht kann nur übergangsweise helfen

Diese verfassungsrechtlichen Grundsätze gelten auch in einer Pandemie. Exekutives Recht kann hier allenfalls in einer Notsituation übergangsweise ein probates Instrument sein. Je länger aber grundrechtliche Belastungen andauern, desto wichtiger ist die Einbindung des originär verantwortlichen parlamentarischen Gesetzgebers.

Während die Landesregierung in dieser Sache nicht aktiv wurde, hat sich der Bundesgesetzgeber mittlerweile der Angelegenheit angenommen und mit Gesetz vom 18. November 2020 die erforderliche Rechtsgrundlage zur Kontaktdatenerhebung geschaffen (§ 28 a Infektionsschutzgesetz). Ich begrüße dies ausdrücklich, da hierdurch die erforderliche Rechtssicherheit geschaffen wird.

Kontaktdaten datenschutzkonform erheben

Die Erhebung der Kontaktdaten gestaltete sich für die betroffenen Betriebe und Einrichtungen nicht immer einfach, da einige datenschutzrechtlichen Voraussetzungen erfüllt werden müssen. Zunächst muss die Vertraulichkeit nach Art. 5 Abs. 1 lit. f) DS-GVO gewahrt sein. Vertraulichkeit bedeutet, dass die personenbezogenen Daten, die erhoben werden, ausschließlich von den jeweiligen Gewerbebetrieben und Bildungseinrichtungen verarbeitet und abgesehen davon an keine weiteren dritten Personen übermittelt werden. Eine Ausnahme bildet in diesem Fall das Gesundheitsamt, da dieses die besagten personenbezogenen Daten zur Kontaktnachverfolgung benötigt.

1 Saarländ. VerfGH (Lv 15/20)

2 BVerfGE 65, 1 (Volkszählung)

Einzelne Zettel sind besser als eine lange Liste

Häufig wurden aber offene Listen geführt, in denen zahlreiche Einträge untereinander standen. Somit konnten beispielsweise Restaurantgäste sehen, wer vor ihnen im Restaurant war. Solche Listen sind dementsprechend nicht vertraulich. Im schlechtesten Fall könnten andere Personen auf den Einfall kommen, das Smartphone zu zücken und ein Foto von den Listen zu fertigen. Eine datenschutzkonforme Variante, mit der sich die Vertraulichkeit wahren lässt, wäre die Erfassung der Kontaktdaten über Einzelblätter. Diese können von jeder Kundin oder jedem Kunden selbst ausgefüllt, durch Verantwortliche eingesammelt und sicher verwahrt werden, so dass keine Drittpersonen Zugriff auf diese Daten erhalten.

Transparenz

Hinweise und Muster zur Datenerhebung: https://t1p.de/corona-daten

Bei der Erhebung der Kontaktdaten ist der Verantwortliche zudem in der Pflicht nach Art. 12 Abs. 1 S. 1 DS-GVO transparent zu informieren. Die Betroffenen müssen in Kenntnis gesetzt werden, zu welchem Zweck, welche Art von Daten in welchem Umfang erhoben werden, mit welcher Berechtigung sie verarbeitet werden, an wen sie übermittelt und zu welchem Zeitpunkt sie fristgemäß gelöscht werden, wenn sie nicht mehr benötigt werden. Diese Informationen müssen zudem in einer einfach verständlichen Sprache gehalten sein. Meine Behörde hat direkt zum Geltungsbeginn der entsprechenden Regelungen in der Corona-VO Muster für Betriebe und Einrichtungen veröffentlicht, mit denen diese Informationspflichten erfüllt werden können.

Datensparsamkeit und Zweckbindung

Verpflichtend erhoben werden durften zudem nur die in der Corona-VO geforderten Daten: Familienname, Vorname, vollständige Anschrift, Telefonnummer sowie Erhebungsdatum und -uhrzeit. Falls auch die E-Mail-Adresse erhoben wird, muss deutlich werden, dass es sich dabei um eine freiwillige Angabe handelt. Der Betrieb oder die Einrichtung darf die Daten keinesfalls für geschäftliche oder private Zwecke nutzen wie Werbeanschreiben oder eine private Kontaktanbahnung.

Datensicherheit

Außerdem müssen Betriebe und Einrichtungen die Sicherheit der erhobenen Daten nach Art. 5 Abs. 1 lit. f) DS-GVO gewährleisten. Das bedeutet, dass diese nicht offen für jedermann zugänglich sein dürfen, sondern jedes Schriftstück, welches personenbezogene Daten enthält, an einem sicheren Aufbewahrungsort verwahrt wird, zu dem kein Unberechtigter Zutritt hat.

Datenlöschung

Keine Dokumente ins Altpapier

Die Kontaktdaten müssen laut Corona-VO nach spätestens einem Monat gelöscht oder datenschutzkonform vernichtet werden. Das bedeutet, dass beispielsweise Papierakten nicht im Altpapier entsorgt werden dürfen sondern durch einen Schredder der Sicherheitsstufe drei bis vier besitzt, zerstört werden müssen.

Beratung hat sich bewährt

Im Jahr 2020 gingen rund 200 Eingaben zum Umgang mit Corona-Listen bei mir ein, darunter knapp 130 Beschwerden. Ich war in diesen Fällen überwiegend beratend tätig und habe den jeweiligen Unternehmen einen konkreten Hinweis zur datenschutzkonformen Führung der Kontaktlisten erteilt. Dabei habe ich die jeweiligen Unternehmen zugleich darauf hingewiesen, ein aufsichtsbehördliches Überprüfungsverfahren einzuleiten, sofern mich weitere Beschwerden über deren nicht-datenschutzkonformen Umgang mit der Erhebung der Kontaktdaten erreichen würden. Dieses Vorgehen hat sich in der Praxis bewährt. Das wurde auch daran deutlich, dass mich keine zweite Beschwerde gegen dasselbe Unternehmen zum Umgang mit Kontaktdaten erreichte. Vielmehr wurden die Hinweise offenbar von den jeweiligen Unternehmen angenommen und in die Tat umgesetzt.

1.2 Übermittlung von Corona-Quarantänelisten an die Polizei

Zu Beginn der Corona-Pandemie sollten die niedersächsischen Gesundheitsämter tagesaktuell die Listen aller Personen, die sich in Quarantäne befanden, an die örtlichen Polizeileitstellen übermitteln. Dies stellte eine unrechtmäßige Datenübermittlung auf Vorrat dar.

Pressemitteilung zur Datenübermittlung durch Gesundheitsämter: https://t1p.de/pm-quarantaenelisten

Das Niedersächsische Sozialministerium forderte die Gesundheitsämter im April 2020 per Runderlass auf, die Daten sämtlicher sich in Quarantäne befindlichen Personen an die örtlichen Polizeileitstellen zu übersenden. Begründet wurde dies mit dem Eigenschutz der Einsatzkräfte, da zu diesem Zeitpunkt noch keine Schutzausrüstung in ausreichender Menge vorhanden war. Diesen Erlass habe ich beanstandet und seine Aufhebung gefordert, da es keine Rechtsgrundlage für die Übermittlung der besonders schutzwürdigen Daten der betroffenen Personen gab.

Nachdem sich das Sozialministerium zunächst geweigert hatte, den Erlass aufzuheben, wurde von dort im Frühsommer die Schaffung einer Rechtsgrundlage angekündigt. Allerdings äußerte ich Bedenken im Hinblick auf die Verhältnismäßigkeit einer gesetzlichen Regelung. Das Sozialministerium sah schließlich von seinem Vorhaben ab und hob den streitigen Runderlass auf.

Die Übermittlung der Daten sämtlicher sich in Quarantäne befindlichen Personen ist eine anlasslose Vorratsdatenverarbeitung sensitiver Gesundheitsdaten. Denn eine Quarantäne darf nach den Regelungen des Infektionsschutzgesetzes nur angeordnet werden, wenn der Verdacht einer Erkrankung oder einer Übertragung mit dem Coronavirus besteht. Es handelt sich hier um eine Übermittlung besonders schutzwürdiger Gesundheitsdaten, die nur unter den engen Voraussetzungen des Art. 9 Abs. 2 Datenschutz-Grundverordnung verarbeitet werden dürfen. Hierfür bietet aber weder § 41 Nds. Polizeigesetz noch der Runderlass des Sozialministeriums die erforderliche fachspezifische Rechtsgrundlage.

Ich halte es grundsätzlich für problematisch, dass die ohnehin stark belasteten Gesundheitsämter in der Pandemie einander widersprechende Rechtsvorgaben zweier Aufsichtsbehörden erhalten. Da der Vorgang aber auch überregional mit großer Verwunderung zur Kenntnis genommen wurde, gehe ich davon aus, dass das Sozialministerium künftig meinen datenschutzrechtlichen Hinweisen frühzeitig Rechnung tragen wird.

1.3 Corona-Warn-App mit Datenschutz von Anfang an

Mit Beginn der Corona-Pandemie wurden große Hoffnungen auf die Corona-Warn-App gesetzt. Diese sollte der digitalen Kontaktverfolgung durch Bürgerinnen und Bürger dienen, um Infektionsketten so schnell wie möglich nachverfolgen und unterbrechen zu können. Bereits in der Entwicklungsphase kam dem Datenschutz eine hohe Bedeutung zu.

Ende April 2020 teilte die Bundesregierung mit, dass die Corona-Warn-App federführend von der Deutschen Telekom und dem Software-Konzern SAP entwickelt und zur Marktreife gebracht werden soll. Die Fraunhofer-Gesellschaft und das Helmholtz-Zentrum für Informationssicherheit gGmbH waren beratend tätig. Um die Anforderungen an Datenschutz und IT-Sicherheit zu gewährleisten, waren zudem der Beauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und das Bundesamt für die Sicherheit in der Informationstechnik (BSI) von Beginn an in die Entwicklung der App eingebunden. Herausgeber und Betreiber der App ist das Robert-Koch-Institut. Sie ist seit dem 16. Juni 2020 in Deutschland und seit Anfang Juli 2020 auch in allen Staaten der EU verfügbar.

Funktionsweise der App

Bürgerinnen und Bürger können die Corona-Warn-App in den App-Stores kostenlos herunterladen, sofern ihre mobilen Endgeräte bestimmte technische Voraussetzungen erfüllen. Die App verfügt über die vier Hauptfunktionen:

- Risiko-Ermittlung
- Meldung des positiven Corona-Tests
- Risikobewertung sowie
- Information und Handlungsempfehlung.

Smartphones tauschen Zufalls-IDs

Über die Bluetooth-Technik erkennen sich Smartphones gegenseitig, auf denen die App installiert ist und die sich innerhalb eines näheren Umkreises (max. zehn Meter) befinden. Erfolgt der Kontakt (der Smartphones) nach Abstand und Zeitdauer für einen risikorelevanten Zeitraum, tauschen die Geräte Zufalls-IDs aus, die jeweils in der App des Nutzers oder der Nutzerin für 14 Tage gespeichert werden. Die Zufalls-ID wird aus einer ebenfalls zufälligen Geräte-ID abgeleitet.

Sind Nutzerinnen oder Nutzer der App positiv auf das Corona-Virus getestet worden, können sie diese Information und ihre eigenen Geräteschlüssel zum Abgleich freiwillig mitteilen. Der Geräteschlüssel wird dann auf dem Corona-Warn-App-Server gespeichert. Anschließend werden alle Zufalls-IDs des oder der Infizierten der letzten 14 Tage, versehen mit dem Gültigkeitstag und dem „Übertragungsrisiko“, auf dem Server für alle Nutzerinnen und Nutzer der Corona-Warn-App verfügbar gemacht. Alle aktiven Corona-Warn-Apps laden regelmäßig die auf dem Server veröffentlichten sogenannten Positivkennungen herunter; auf dem Smartphone wird geprüft, ob gespeicherte Zufallscodes vorliegen, die dem Zufallscode der positiv auf SARS-CoV-2 getesteten Person entsprechen.

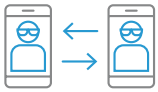
Bei einem positiven Ergebnis des Abgleichs werden die Nutzerinnen und Nutzer über die App in zwei Stufen gewarnt. Fand der Kontakt in einem geringen Umfang statt, wird lediglich ein geringes Risiko ausgewiesen. Wenn die Nutzerin oder der Nutzer in gefährdendem Umfang Kontakt zu einer infizierten Person hatte, erhält sie oder er dagegen eine rote Warnung und es wird empfohlen, zu Hause zu bleiben, Begegnungen mit anderen zu vermeiden und auf mögliche Symptome zu achten.

So funktioniert die Corona-Tracing-App

Auf **freiwilliger** Basis können Menschen die App auf dem Smartphone **installieren**.

Jede App generiert regelmäßig **anonyme Kurzzeit-IDs** und sendet diese via Bluetooth in die Umgebung.

Via **Bluetooth** erkennt die App andere Smartphones in der Nähe, die die App ebenfalls installiert haben.



Befinden sich zwei Smartphones für z. B. **15 Minuten unter 1,5 m** beieinander, werden die IDs ausgetauscht.

IDs von Kontaktpersonen werden **lokal** auf dem Smartphone gespeichert. Die App speichert **keine Bewegungsdaten oder persönlichen Informationen**.

Bei **festgestellter Infektion** durch einen Arzt meldet der User dies via Scan eines QR-Codes, den er vom Arzt oder Labor erhält.* Anonyme IDs der Infizierten werden an Server übermittelt.

Anonyme **IDs der Infizierten** werden min. ein Mal am Tag auf alle Geräte übermittelt. Der **Datenabgleich** findet dann **lokal** statt.

Kontaktpersonen des Infizierten werden dann **per Push-Mitteilung benachrichtigt** und können Maßnahmen ergreifen.

*Eintrag einer Infektion alternativ auch über Telefon-Hotline

dpa•101063 Quelle: SAP, Deutsche Telekom

Datenschutzkonforme Gestaltung

Aus der Politik kam während des ersten Lockdowns im Frühjahr 2020 die Forderung, dass eine auf Standortdaten basierende Corona-Warn-App entwickelt werden sollte, mit der jeder Nutzer und jede Nutzerin nachverfolgt werden kann. Hiergegen hat unter anderem der Europäische Datenschutzausschuss (EDSA) in den am 22. April 2020 veröffentlichten Leitlinien 04/2020 für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19 datenschutzrechtliche Bedenken geäußert. In den Guidelines finden sich darüber hinaus umfassende datenschutzrechtliche Empfehlungen und Funktionsanforderungen. Die Verwendung von Standortdaten wurde anschließend verworfen, da keine praktische Notwendigkeit für ein umfassendes Tracking besteht.

Leitlinien 04/2020 des EDSA: https://t1p.de/edsa-standort

Dezentral statt zentral

Zu Beginn der Pandemie verfolgte eine europäische Initiative – die „Pan-European Privacy-Preserving Proximity Tracing" (PEPP-PT) – zur Entwicklung einer Basistechnologie, der sich auch die Bundesregierung angeschlossen hatte, eine zentrale Datenspeicherung der Kontakte. Gleichzeitig entstand unter anderem unter Mitarbeit des Helmholtz-Zentrums für Informationssicherheit die alternative Softwarearchitektur DP-3T (Decentralized Privacy-Preserving Proximity Tracing), mit der ein dezentrales Konzept verfolgt wurde. Nachdem sich erheblicher Widerstand gegen die zentrale Methode von PEPP-PT geregt hatte, wandten sich die deutsche und viele weitere Regierungen von dem zunächst befürworteten zentralen Modell ab und verfolgten den dezentralen Ansatz, der deutlich datenschutzfreundlicher ist. Auch das europäische Parlament befürwortete den dezentralen Ansatz ausdrücklich.[1]

Open-Source-Ansatz

Die Deutsche Telekom und SAP entwickelten die Corona-Warn-App als Open-Source-Produkt und veröffentlichten Mitte Mai ein erstes Konzept für die deutsche App. Aus datenschutzrechtlicher Sicht bietet eine Open-Source-Software eine hohe Transparenz und ist daher zu begrüßen. Zudem ist diese Vorgehensweise mit dem Vorteil verbunden, dass viele Experten die Software analysieren und gegebenenfalls Fehler aufspüren können.

Mit dem Start der Corona-Warn-App im Juni 2020 wurde auch die gemäß Art. 35 DS-GVO erforderliche Datenschutz-Folgenabschätzung für die App veröffentlicht, die zuvor vom BfDI mit positivem Ergebnis geprüft worden war.

Stellungnahmen der Datenschutzaufsicht

Pressemitteilungen der DSK: https://t1p.de/pm-dsk

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) begleitete den Start der Corona-Warn-App mit einer Pressemeldung. Darin wurde einerseits das datenschutzfreundliche Grundkonzept der Corona-Warn-App ausdrücklich gelobt. Andererseits wurde auf die Gefahr hingewiesen, dass die Freiwilligkeit der App-Nutzung nicht untergraben werden dürfe.

Aufgrund der besonderen gesellschaftlichen Bedeutung der Corona-Warn-App habe auch ich eine Pressemitteilung zu deren Start veröffentlicht. Mir war es ein besonderes Anliegen, das hohe Maß an datenschutzrechtlicher Transparenz und die Bedeutung der freiwilligen Nutzung der App noch einmal deutlich zu betonen.

Pressemitteilung der LfD Niedersachsen: https://t1p.de/pm-warn-app

Ich sehe die Corona-Warn-App als Musterbeispiel dafür, dass das Prinzip Privacy by Design (Datenschutz durch Gestaltung) erstens realisierbar ist und zweitens einen sehr effizienten und effektiven Weg für die Gewährleistung des Datenschutzes darstellt. Der oben dargestellte Verlauf macht deutlich nachvollziehbar, dass zu mehreren Zeitpunkten während der Planung und Entwicklung wichtige Entscheidungen im Sinne datenschutzförderlicher Technikgestaltung getroffen worden sind. Der öffentliche Diskurs und die stetige Beteiligung der Aufsichtsbehörden haben letztlich dazu geführt, dass wir eine datenschutzkonforme Corona-Warn-App nutzen können.

1 Entschließung des Europäischen Parlaments vom 17. April 2020: https://t1p.de/eu-parla-corona

1.4 Datenschutzkonforme Nachweise zur Befreiung von der Maskenpflicht

Nach der Niedersächsischen Corona-Verordnung (CoronaVO) kann man sich mit einem entsprechenden Nachweis von der Pflicht zum Tragen einer Mund-Nasen-Bedeckung befreien lassen. Zu diesem Thema erhielt ich zahlreiche Eingaben, besonders aus dem Bereich der Schulen und der Kindertagesstätten.

Die Maskenpflicht der Schülerinnen und Schüler in den niedersächsischen Schulen ist in den §§ 3 und 13 CoronaVO[1] geregelt. Gemäß § 3 Abs. 6 CoronaVO sind Personen, für die aufgrund einer körperlichen, geistigen oder psychischen Beeinträchtigung oder einer Vorerkrankung das Tragen einer Mund-Nasen-Bedeckung nicht zumutbar ist und die dies durch ein ärztliches Attest oder eine vergleichbare amtliche Bescheinigung glaubhaft machen, von dieser Verpflichtung ausgenommen. In der Praxis wurde oft ein ärztliches Attest verlangt, welches eine Diagnose enthält. Zudem wurden häufig Kopien der Atteste zu den Akten genommen. Dies wurde vielfach beanstandet.

So viel wie nötig, so wenig wie möglich

Erlasse machen einheitliche Vorgaben für Atteste

Im Rahmen von Runderlassen machte die Niedersächsische Landesschulbehörde im Oktober und November 2020 einheitliche Vorgaben für den Inhalt von Attesten zur Befreiung von der Maskenpflicht im Schulbereich. Demnach sind Symptombeschreibungen erforderlich, die durch einen Arzt festgestellt wurden. Zudem müssen relevante Vorerkrankungen benannt werden. Diese Vorgaben seien erforderlich, um Gefälligkeitsatteste ausschließen zu können. Eine Kopie des Attestes darf jedoch nicht zur Schülerakte genommen werden.

Klarheit durch Rechtsprechung

Die CoronaVO selbst trifft zwar keine Aussage zu den Inhalten der Atteste, mit denen sich Personen von der Maskenpflicht befreien lassen können. Jedoch liegen zu dieser Frage bereits mehrere obergerichtliche Entscheidungen vor.

So hat das Oberverwaltungsgericht für das Land Nordrhein-Westfalen am 24. September 2020 (Az: 13 B 1368/20) entschieden, dass es für eine glaubwürdige Ausnahmeregelung in Bezug auf die Maskenpflicht eines aussagekräftigen ärztlichen Attestes bedarf. Dieses muss kurzfristig erwartbare gesundheitliche Beeinträchtigungen konkret benennen und vorliegende relevante Vorerkrankungen konkret bezeichnen.

Ebenfalls hat der Bayerische Verwaltungsgerichtshof durch Beschluss vom 26. Oktober 2020 (Az.: 20 CE 20.2185) entschieden, dass ein Attest nachvollziehbare Befundtatsachen sowie eine Diagnose enthalten muss.

1 Diese Verordnung stützt sich auf § 28 a Absatz 1 Nr. 2 Infektionsschutzgesetz.

Das Oberverwaltungsgericht Rheinland-Pfalz hat diese Vorgaben durch Beschluss vom 20. November 2020 für den Bereich der Ausnahmen von der Präsenzpflicht bestätigt (Az: 2 B 11333/20) und auf den komplexen Abwägungsprozess verwiesen, den die Schulleitung auf der Grundlage der Grundentscheidung des Landes für den Präsenzunterricht zu treffen hat.

Schließlich hat sich mit dem Verwaltungsgericht Lüneburg auch ein niedersächsisches Gericht mit Beschluss vom 3. Dezember 2020 (Az: 6 B 126/20) in Bezug auf die Maskenpflicht für Lehrkräfte den genannten obergerichtlichen Entscheidungen zur Ausgestaltung von Attesten angeschlossen.

Bedenken zurückgestellt

Kopie ist nicht zulässig

Vor diesem Hintergrund habe ich meine anfänglichen Bedenken im Hinblick auf Detailangaben im Attest zurückgestellt und die Eingaben im Sinne der Rechtsauffassung des Niedersächsischen Kultusministeriums beantwortet. Die Anfertigung einer Kopie zur Aufnahme in die Schülerakte ist allerdings nicht datenschutzkonform. Ein Aktenvermerk, dass ein entsprechendes Attest vorgelegt wurde, reicht aus.

1.5 Einsatz von SORMAS in den Gesundheitsämtern

Der Ausbruch der Corona-Pandemie im Frühjahr 2020 führte zu einem nicht mehr zu bewältigendem Anstieg der Arbeit in den Gesundheitsämtern. Für Entlastung sollte das Programm SORMAS[1] sorgen, eine Entwicklung des Helmholtz-Zentrums für Infektionsforschung (HZI). In einem speziell entwickelten Coronavirus-Modul für den öffentlichen Gesundheitsdienst können zu den betroffenen Personen neben klinischen und diagnostischen Parametern der Covid-19-Erkrankung auch Kontaktpersonen erfasst und nachverfolgt werden.

Die Aufgaben und Pflichten nach dem Infektionsschutzgesetz (IfSG) obliegen in Niedersachsen den Gesundheitsämtern. Die Meldewege nach dem IfSG und die gesetzlichen Aufgaben im Rahmen der Nachverfolgung der von einer meldepflichtigen Infektion betroffenen Person sowie deren Kontaktpersonen gehörte bereits vor dem Jahr 2020 zur täglichen Arbeit der Gesundheitsämter.

Gesundheitsamt darf Ermittlungen anstellen

Ein Gesundheitsamt ist nach § 28 IfSG befugt Schutzmaßnahmen zu erlassen, soweit und solange es zur Verhinderung der Verbreitung übertragbarer Krankheiten erforderlich ist. Nach § 25 Abs. 1 IfSG ist das Gesundheitsamt auch befugt, erforderliche Ermittlungen, insbesondere über Art, Ursache, Ansteckungsquelle und Ausbreitung der Krankheit anzustellen. Diese Maßnahmen betreffen neben den Erkrankten auch Kontaktpersonen.

Bedeutung von Gesundheitsdaten

Die in den Gesundheitsämtern zu verarbeitenden Daten betreffen den Gesundheitszustand von Menschen. Sie gehören damit zu den besonders sensiblen Daten, mit denen im Missbrauchsfall durch unbefugte Dritte ein sehr hoher Schaden für die Gesundheit oder das Ansehen der betroffenen Person entstehen kann. Aus diesem Grund dürfen in den Gesundheitsämtern nur Programme eingesetzt werden, welche die datenschutzrechtlichen Anforderungen erfüllen.

Anfrage des Sozialministeriums zu SORMAS

In Vertretung für die einzelnen Gesundheitsämter legte mir das Niedersächsische Ministerium für Soziales, Gesundheit und Gleichstellung (MS) bereits Ende Mai 2020 eine Vielzahl von Unterlagen des HZI zu SORMAS zur Prüfung vor. Die Dokumente befanden sich in einem sehr frühen Stadium und waren dementsprechend noch nicht aussagkräftig genug, um eine abschließende datenschutzrechtliche Bewertung des vollständigen Programms mit allen Erweiterungen vornehmen zu können.

1 Surveillance Outbreak Response Management and Analysis System

Lokale Freigabe für SORMAS

Im Rahmen meiner Prüfung kam ich zu dem Ergebnis, dass der Betrieb von SORMAS lokal auf den eigenen IT-Systemen des jeweiligen Gesundheitsamtes datenschutzgerecht möglich ist. Anfang Juni übersandte ich meine datenschutzrechtliche Bewertung zusammen mit Überarbeitungs- und Verbesserungsvorschlägen an das MS. Zugleich stimmte ich dem lokalen Betrieb von SORMAS in den Gesundheitsämtern innerhalb des eigenen örtlichen Zuständigkeitsbereichs unter dem Vorbehalt der Umsetzung meiner datenschutzrechtlichen Anmerkungen zu, damit die Ämter so schnell wie möglich entlastet werden konnten.

Integriertes Symptom-Tagebuch

Wie bereits erwähnt, müssen die Gesundheitsämter nicht nur Maßnahmen gegenüber infizierten Personen erlassen und nachhalten, sondern vor allem auch gegenüber den Personen, mit denen die infizierte Person zuvor in Kontakt gestanden hat. Durch die Nachverfolgung der Kontakte können Infektionsketten nachvollzogen, unterbrochen und so die Ausbrüche eingedämmt werden. Das Robert-Koch-Institut (RKI) hat Definitionen für eine Kategorisierung der Kontaktpersonen nach deren Infektionsrisiko herausgegeben. Personen, die länger als 15 Minuten engen Kontakt ohne angemessenen Schutz zu einer infizierten Person hatten, werden vom Gesundheitsamt als K1 eingestuft. Diese Personengruppe muss für 14 Tage mindestens einmal täglich vom Gesundheitsamt zu ihrem Gesundheitsstatus befragt werden. In der Regel geschieht dies telefonisch, was einen immensen personellen Aufwand für die Gesundheitsämter darstellt.

Definitionen der Kontaktpersonen: https://t1p.de/rki-kontaktpersonen

Es wurde daher ebenfalls beabsichtigt, das Programm SORMAS um ein digitales Symptom-Tagebuch zu erweitern. Das entweder als Web-App oder mobile App konzipierte Tagebuch sollte einerseits die Anzahl der zu führenden Telefonate um ein Vielfaches reduzieren und andererseits den Kontaktpersonen die Möglichkeit eröffnen, selbst zu bestimmen, wann ihre Angaben an das Gesundheitsamt übermittelt werden.

Die Kontaktpersonen sind zwar zur Mitwirkung gegenüber dem Gesundheitsamt verpflichtet, die Nutzung des Symptom-Tagebuchs ist hingegen ein freiwilliges Angebot, dessen Nutzung jederzeit ohne Angabe von Gründen oder Nachteilen beendet werden kann. Anhand der mir hierzu vorgelegten Unterlagen habe ich auch den Einsatz dieses Programms akzeptiert.

Tagebuch soll zu weniger Telefonaten führen

Weiterentwicklung von SORMAS

Zum Zeitpunkt meiner Prüfung wurde bereits darauf hingewiesen, dass das Programm SORMAS in zukünftigen Versionen auch Schnittstellen für die verpflichtende Datenübermittlung an das RKI oder im Falle des Wechsels der Zuständigkeit die Übermittlung der gespeicherten Falldaten an andere Gesundheitsämter ermöglichen kann. Es soll ebenfalls möglich sein, dass Daten aus Symptom-Tagebüchern anderer Anbieter in SORMAS verarbeitet werden können.

Mit Beginn der zweiten Welle der Pandemie Ende 2020, die noch einmal eine deutlich höhere Zahl der täglich positiv getesteten Personen und eine entsprechend höhere Zahl der Kontaktpersonen mit sich brachte, wurde ein bundesweiter Einsatz von SORMAS diskutiert und vom Bundes-

Bundesweiter Einsatz gewünscht

ministerium für Gesundheit initiiert. Die Federführung für die datenschutzrechtliche Bewertung übernahm der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), der die Länder entsprechend beteiligte.

Die zum Ende des Berichtsjahres vorgelegten Dokumente zu SORMAS, inklusive der genannten Weiterentwicklungen, waren bereits nahezu vollständig. Eine abschließende datenschutzrechtliche Bewertung lag zum Ende des Berichtszeitraums noch nicht vor. Niedersachsen hat bereits Anfang Juni 2020 den Einsatz von SORMAS lokal und des Symptom-Tagebuchs ermöglicht. Mit Schreiben vom 18. Januar 2021 an das BMG hat auch der BfDI den Einsatz von SORMAS und der Weiterentwicklungen unter dem Vorbehalt der Ergänzungen des Datenschutzkonzepts sowie Klärung der verbleibenden Rechtsfragen für zulässig erklärt.

1.6 Einlass ins Rathaus nur gegen Gesundheitsdaten

Nach dem ersten Lockdown im Frühjahr 2020 hat eine Stadt in Niedersachsen für den Zutritt zu öffentlichen Einrichtungen neben Kontaktdaten auch Angaben zur Gesundheit von Bürgerinnen und Bürgern abgefragt. Ohne eine Antwort auf die Fragen, wurde der Zugang verweigert.

Durch einen Pressebereicht wurde ich im Mai 2020 auf das Vorgehen der Stadt aufmerksam. Ich schrieb die Stadtverwaltung daraufhin an und bat um Erläuterungen. Aus datenschutzrechtlicher Sicht war von besonderer Bedeutung, auf welche Rechtsgrundlage die Datenerhebung gestützt wurde und für welchen Zeitraum die erhobenen personenbezogenen Daten gespeichert wurden.

Verfahren war bereits angepasst

Keine Fragen mehr zu Gesundheit und Reisen

Die Stadt teilte mir mit, dass aufgrund neuerer Erkenntnisse über das Corona-Virus die ursprüngliche Speicherdauer von sechs Wochen auf drei bis vier Wochen verkürzt worden sei. Ferner werde auf die zusätzlichen Fragen (z. B. Leiden Sie an akuten Atemwegsbeschwerden? Waren Sie in den vergangenen zwei Wochen im Ausland?) verzichtet. Zweck der Verarbeitung sei es, im Bedarfsfall Infektionsketten nachverfolgen zu können. Nur mit der Erhebung sei es möglich, öffentliche Einrichtungen wieder zu öffnen.

Nur freiwillige Auskunft ist zulässig

Doch auch für die Verarbeitung der Kontaktdaten der Bürgerinnen und Bürger existierte zum damaligen Zeitpunkt keine Rechtsgrundlage. Das Land Niedersachsen hatte in der Niedersächsischen Corona-Verordnung Bereiche vorgegeben, in denen Kontaktdaten erhoben werden mussten. Öffentliche Einrichtungen waren zunächst nicht von dieser Pflicht erfasst. Aus diesem Grund war es nicht zulässig, beispielsweise den Besuch des Rathauses oder der Bibliothek von der Angabe von Kontaktdaten abhängig zu machen. Als Grundlage für die Datenverarbeitung kam somit nur eine Einwilligung der betroffenen Personen in Betracht. Diese setzt jedoch die Freiwilligkeit voraus. Diese liegt vor, wenn die Datenangabe ausschließlich im eigenen Interesse der Bürgerinnen und Bürger erfolgt, also auch ohne Ausfüllen eines Kontaktformulars der Zugang zu einer öffentlichen Einrichtung gewährt wird.

Rechtsgrundlage kam im September 2020

Behörden dürfen Kontaktdaten erheben

Im September 2020 passte das Land Niedersachsen seine Corona-Verordnung an, sodass nun Behörden aufgrund der örtlichen Gegebenheiten entscheiden konnten, ob sie Kontaktdaten im Sinne der Verordnung erheben. Die Erhebung zusätzlicher Daten, zum Beispiel zum Gesundheitszustand, ist weiterhin nicht zulässig.
Die betroffene Kommune habe ich zwischenzeitlich verwarnt, insbesondere wegen der zeitweise zusätzlich gestellten Fragen zum Gesundheitszustand und zum Reiseverhalten der Bürgerinnen und Bürger.

1.7 Übermittlung von Gästedaten vor der Ankunft

Zwei Landkreise haben per Allgemeinverfügung Beherbergungsbetriebe angewiesen, bereits vor der Ankunft von Gästen Kontaktdaten zu erheben und an die Kommunalverwaltung zu übermitteln. Hierzu gingen mehrere Eingaben ein.

Im Mai 2020 erließen zwei Landkreise zur Bekämpfung der Corona-Pandemie befristete Allgemeinverfügungen, die vorsahen, dass Kontaktdaten zukünftiger Gäste von zum Beispiel Ferienwohnungen bereits vor der Ankunft zu erheben und an die Stadt- bzw. Gemeindeverwaltung zu übermitteln sind. Das sollte im Falle eines Corona-Ausbruches die Nachverfolgung von Infektionsketten ermöglichen. Für andere Unternehmen, wie zum Beispiel Restaurants, sah die Niedersächsische Corona-Verordnung zu diesem Zeitpunkt ebenfalls die Erhebung von Kontaktdaten vor. Die nach der Verordnung erhobenen Kontaktdaten mussten jedoch nur auf Anforderung an das Gesundheitsamt übermittelt werden und nicht an die Stadt- bzw. Gemeindeverwaltung.

Keine Datenerhebung vor der Ankunft

Ich wies die Landkreise darauf hin, dass die Erhebung von Kontaktdaten der Gäste vor deren Ankunft aus datenschutzrechtlicher Sicht nicht zulässig ist. Den Landkreisen wurde Gelegenheit gegeben, mir ihr Vorgehen zu erläutern und Änderungen an der Allgemeinverfügung vorzunehmen. Ein Kreis hob seine Allgemeinverfügung auf und erließ eine neue, datenschutzgerechte Fassung. Diese war zeitlich befristet und trat nach Firstablauf automatisch außer Kraft.

Verfügungen werden aufgehoben bzw. nicht verlängert

Der andere Landkreis kündigte zunächst an, die Allgemeinverfügung in unveränderter Form zu verlängern. Aus diesem Grund nahm ich mit den von der Datenverarbeitung betroffenen Gemeinden Kontakt auf, da diese im datenschutzrechtlichen Sinne Verantwortliche für die Verarbeitung der übermittelten Kontaktdaten waren. Aufgrund meiner Kontaktaufnahme wurden die bereits übermittelten Gästedaten gelöscht und die Verarbeitung beendet. Der Landkreis verlängerte seine ebenfalls befristete Allgemeinverfügung nicht.

1.8 Nutzung digitaler Kommunikationsmittel durch Schulen und Hochschulen

Die Corona-Pandemie hat die Digitalisierung im Bildungsbereich beschleunigt, zugleich aber auch die Schwächen im System offengelegt. Die verantwortlichen Stellen tragen die Verantwortung für die Auswahl datenschutzkonformer Produkte, um eventuelle Risiken für die Grundrechte der Betroffenen auszuschließen. Schulen und Hochschulen sind auch in der Pandemie gefordert, datenschutzkonforme digitale Bildungsangebote zu machen.

Zu Beginn der Corona-Pandemie hatte ich zeitlich begrenzt geduldet, dass öffentliche Stellen auch solche digitalen Kommunikationsmittel – wie Videokonferenz- und Clouddienste – einsetzen dürfen, die nicht im vollen Umfang sämtliche datenschutzrechtlichen Anforderungen erfüllen. Mit diesem Zugeständnis wollte ich meinen Teil dazu beitragen, dass den Schülerinnen und Schülern sowie den Studierenden wegen der Einrichtungsschließungen zügig digitale Bildungsangebote gemacht werden konnten. Nachdem die Verantwortlichen hinreichend Zeit hatten, die Datenschutzkonformität der eingesetzten Produkte sicherzustellen, habe ich meine Duldung im Herbst 2020 widerrufen.

Das bedeutet, dass Verantwortliche bereits vor der Verarbeitung der personenbezogenen Daten sicherstellen müssen, dass die eingesetzten Produkte datenschutzkonform sind. Ich habe das Niedersächsische Kultusministerium, das Niedersächsische Ministerium für Wissenschaft und Kultur sowie das Niedersächsische Ministerium für Soziales, Gesundheit und Gleichstellung im Oktober 2020 gebeten, ihre jeweils nachgeordneten Bereiche entsprechend zu informieren.

1.9 Unzulässige Vorratsdatenübermittlung ans Krankenhaus

Ein Gesundheitsamt übermittelte einem örtlichen Krankenhaus personenbezogene Daten aller positiv auf das Corona-Virus getesteten Personen. Dies sollte die Ausbreitung von Infektionen innerhalb des Krankenhauses verhindern.

Gegen Jahresende wurde mir von einem Gesundheitsamt eine Datenschutzverletzung gemeldet. Es hatte versehentlich unverschlüsselt personenbezogene Daten von positiv auf das Corona-Virus getesteten Personen an das örtliche Krankenhaus übermittelt. Ergänzend wurde mitgeteilt, dass künftig sichergestellt werde, dass die Übermittlung über einen verschlüsselten Übertragungsweg erfolgt.

Für die erfolgte und weiterhin beabsichtigte Übermittlung vom Gesundheitsamt an das Klinikum ist eine Rechtsgrundlage erforderlich. Aus diesem Grund habe ich bei der Stadtverwaltung nachgefragt, auf welcher gesetzlichen Grundlage und zu welchem Zweck das Krankenhaus die personenbezogenen Daten erhält.

Stadt verweist auf das Infektionsschutzgesetz

Aus Sicht der Stadt sei das Gesundheitsamt verpflichtet, die Daten dem Krankenhaus zur Verfügung zu stellen, um Corona-Infektionen im Krankenhaus zu verhindern. Zur rechtlichen Begründung wurde auf das Infektionsschutzgesetz (IfSG) und das Niedersächsische Datenschutzgesetz verwiesen. Diese würden die Übermittlungen ermöglichen.

Übermittlung aller Daten nicht erforderlich

Die mitgeteilten Rechtsgrundlagen konnten die Offenlegung der Daten allerdings nicht rechtfertigen, da die Tatbestandsvoraussetzungen nicht erfüllt waren. Dies gilt insbesondere für die Erforderlichkeit der Offenlegung aller infizierten Personen gegenüber der Klinik. Bei der Beurteilung ist Folgendes zu berücksichtigen:

1. Nur etwa sieben Prozent der Erkrankten bedürfen eines Krankenhausaufenthaltes (Quelle: Robert-Koch-Institut, Stand 8. Januar 2021). Ein Großteil der von der Datenübermittlung betroffenen Personen dürften also keinen Kontakt mit dem Krankenhaus haben.
2. Personen, denen ihre Erkrankung nicht bekannt ist, werden von der Offenlegung nicht erfasst, dabei dürften diese eine größere Gefährdung für Krankenhäuser darstellen.

Tests für Neuaufnahmen mögliche Alternative

Unabhängig davon müssen Krankenhäuser nach dem IfSG geeignete Maßnahmen treffen, um sich vor der Ausbreitung von Infektionen zu schützen. Eine mögliche Maßnahme könnte die Testung aller neu aufzunehmenden Personen auf das SARS-CoV-2 Virus sein.

Aus diesen Gründen ist die pauschale Übermittlung aller dem Gesundheitsamt bekannten und positiv auf das SARS-CoV-2 Virus getesteten Personen an Krankenhäuser nicht erforderlich. Vor diesem Hintergrund wurde die Stadt verwarnt und aufgefordert zu bestätigen, dass die Offenlegung gegenüber der Klinik künftig unterbleibt. Die Stadt ist dieser Aufforderung nachgekommen.

1.10 Beschäftigtendatenschutz während der Corona-Pandemie

Als Aufsichtsbehörde für den Datenschutz überwache ich auch die Einhaltung der datenschutzrechtlichen Bestimmungen bei der Verarbeitung von Beschäftigtendaten. In der Corona-Pandemie erreichten mich dazu zahlreiche Anfragen.

Im Schwerpunkt ging es bei den Fragen, die mir gestellt wurden, um die Verarbeitung von Gesundheitsdaten der Beschäftigten. Deren Verarbeitung ist grundsätzlich untersagt und nur unter sehr engen gesetzlichen Voraussetzungen erlaubt (Artikel 9 Absatz 1 und Absatz 2 DS-GVO). Dies gilt auch im Rahmen einer Pandemie.

Bei der Verarbeitung von Gesundheitsdaten zur Bekämpfung der Corona-Pandemie ist zu beachten, dass sowohl die Bekämpfung als auch die Entscheidung über die dafür eingesetzten Mittel in erster Linie Aufgaben des Staates sind. Zudem gilt im Datenschutzrecht stets der Grundsatz der Datenminimierung Das bedeutet, die Verarbeitung von personenbezogenen Daten muss auf das für den Verarbeitungszweck – hier die Pandemiebekämpfung – notwendige Maß beschränkt sein. Zur Verarbeitung gehört bereits die Erhebung personenbezogener Daten (Artikel 4 Nummer 2 DS-GVO).

Verarbeitung auf notwendiges Maß beschränken

Regeln zur Verarbeitung von Gesundheitsdaten

Das Gesetz sieht grundsätzlich nicht vor, dass Arbeitgeberinnen und Arbeitgeber zum Zweck der Pandemiebekämpfung Gesundheitsdaten ihrer Beschäftigten verarbeiten dürfen. Vielmehr ist gesetzlich in § 26 Absatz 3 des Bundesdatenschutzgesetzes (BDSG) geregelt, dass Gesundheitsdaten der Beschäftigten vom Arbeitgeber oder der Arbeitgeberin nur verarbeitet werden dürfen, wenn dies

- für Zwecke des Beschäftigungsverhältnisses erfolgt und
- für die Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und
- kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Personen, also der Beschäftigten, am Ausschluss der Verarbeitung überwiegt.

Weiter dürfen Gesundheitsdaten von Beschäftigten nach § 22 Absatz 1 Nummer 1 Buchstabe b BDSG verarbeitet werden, wenn dies zur Feststellung ihrer Arbeitsfähigkeit erforderlich ist. Die in diesem Zusammenhang verarbeiteten Gesundheitsdaten dürfen allerdings nicht von jeder Person verarbeitet werden, sondern von ärztlichem Personal oder durch sonstige Personen, die einer

entsprechenden Geheimhaltungspflicht unterliegen. Darüber hinaus zum Beispiel von Personen, die unter der Verantwortung von den genannten Personen sind, zum Beispiel von Arzthelferinnen und Arzthelfern.

Einwilligung muss freiwillig sein

Im Übrigen dürfen Beschäftigtendaten – und auch deren Gesundheitsdaten – aufgrund einer Einwilligung der betroffenen Beschäftigten verarbeitet werden (§ 26 Absätze 2 und 3 BDSG). Damit die Einwilligung in die Verarbeitung von personenbezogenen Daten gültig ist, muss sie freiwillig erteilt sein. Problematisch ist, dass zwischen Arbeitgeberinnen und Arbeitgebern und ihren Beschäftigten ein Abhängigkeitsverhältnis besteht. Deshalb willigen Beschäftigte in die Verarbeitung ihrer personenbezogenen Daten gegebenenfalls nur ein, weil sie den Verlust ihres Arbeitsplatzes oder andere Nachteile befürchten. Dann aber gilt die Einwilligung als nicht mehr freiwillig erteilt und unwirksam. Das Gesetz sieht in § 26 Absatz 2 BDSG allerdings Beispiele vor, wonach die Einwilligung eines Beschäftigten trotz des Über- und Unterordnungsverhältnisses als freiwillig erteilt gilt:

- Wenn die beschäftigte Person durch die Verarbeitung ihrer personenbezogenen Daten einen rechtlichen Vorteil erhält oder
- wenn die beschäftigte Person durch die Verarbeitung ihrer personenbezogenen Daten einen tatsächlichen Vorteil erhält oder
- wenn Arbeitgeber/-in und beschäftigte Person gleichgelagerte Interessen verfolgen.

Im Rahmen der Corona-Pandemie kann aus meiner Sicht angenommen werden, dass beschäftigte Personen, die in die Verarbeitung ihrer Gesundheitsdaten einwilligen, dies auch freiwillig tun und somit deren Einwilligung rechtswirksam ist – denn sowohl die Arbeitgeber und Arbeitgeberinnen als auch die Beschäftigten verfolgen gleichgelagerte Interessen: die Vermeidung weiterer Ansteckungen mit dem Coronavirus und damit auch die Eindämmung der Pandemie.

Darüber hinaus sind auch Einzelfälle denkbar, in denen Arbeitgeber und Arbeitgeberinnen zu weiteren Zwecken Beschäftigtendaten verarbeiten dürfen. So dürfen zum Beispiel – sofern es keine Gesundheitsdaten sind – personenbezogene Daten zum Zweck der Pandemiebekämpfung gemäß Artikel 6 Absatz 1 Buchstabe d DS-GVO verarbeitet werden, wenn dies zum Schutz lebenswichtiger Interessen der betroffenen Personen oder anderer natürlicher Personen erforderlich ist.

Ein Beispiel: Ein Arbeitgeber oder eine Arbeitgeberin möchte Beschäftigte auch außerhalb der Arbeitszeiten schnell darüber informieren können, dass sie Kontakt zu einem an Covid-19 erkrankten Beschäftigten hatten. Zu diesem Zweck werden die privaten Telefonnummern der Beschäftigten erhoben und außerhalb der Arbeitszeiten, zum Beispiel an Feiertagen für diese Information genutzt.

Fiebermessen erlaubt?

DSK-Beschluss zum Einsatz von Wärmebildkameras: https://t1p.de/Waermebildkameras

Am Anfang der Pandemie erreichten nicht nur mich, sondern auch alle weiteren Aufsichtsbehörden Anfragen, ob Arbeitgeberinnen und Arbeitgeber bei Beschäftigten Temperaturmessungen durchführen dürfen. Darüber hinaus ging es auch um die Art und Weise der Messungen. So beabsichtigten Unternehmen zum Beispiel, für diesen Zweck Wärmebildkameras einzusetzen. Da diese Anfragen an alle Aufsichtsbehörden gleichermaßen gerichtet wurden, erließ die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) am 10. September 2020 einen Beschluss zum „Einsatz von Wärmebildkameras beziehungsweise elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie“.

Zusammenfassend lässt sich feststellen: Nicht alle mit dem Coronavirus infizierten Personen haben eine erhöhte Körpertemperatur, sondern bleiben symptomlos. Daher ist die Temperaturmessung nicht geeignet, um eine mögliche Ansteckung tatsächlich zu verhindern. Weiter sind auch aus datenschutzrechtlicher Sicht mildere Maßnahmen, wie zum Beispiel die Einhaltung der Hygiene- und Abstandsbestimmungen und die anlassbezogene Befragung von Beschäftigten denkbar. Diese Maßnahmen sind gleich wirksam und kommen teilweise, wie zum Beispiel die Hygiene- und Abstandsbestimmungen, vollständig ohne eine Datenerhebung aus.

Unternehmen, die wegen individueller räumlicher Gegebenheiten die Einhaltung der vorgegebenen Abstandsbestimmungen nicht überall auf ihrem Betriebsgelände gewährleisten können, setzen derzeit auch Systeme zur Abstandsmessung ein. Dabei werden die Beschäftigten in Echtzeit durch Kameras gefilmt. Eine Software erkennt, ob die Beschäftigten sich an die Abstandsregelungen halten. Unterschreiten die sie den vorgeschriebenen Abstand, ertönt ein akustisches Signal, um sie darauf hinzuweisen. Die abschließende rechtliche Bewertung dieser Vorgehensweise ist noch nicht abgeschlossen.

Testangebote durch Unternehmen

Darüber hinaus erreichten mich Anfragen, inwieweit Unternehmen selbst ihre Beschäftigten auf Corona testen könnten. Dies ist dann möglich, wenn die Tests zum Beispiel von Betriebsärztinnen und -ärzten durchgeführt werden und die Beschäftigten in die Verarbeitung ihrer in diesem Zusammenhang erhobenen Gesundheitsdaten einwilligen. Wie bereits dargestellt kann aufgrund gleichgelagerter Interessen zwischen Arbeitgeberinnen und Arbeitgebern sowie Beschäftigten angenommen werden, dass die Beschäftigten ihre Einwilligung freiwillig und damit rechtswirksam erteilt haben (§ 22 Absatz 2 Satz 2 BDSG).

Datenpannen in Unternehmen

Im Zusammenhang mit der Corona-Pandemie kam es auch zu vermehrten Meldungen von Datenpannen durch Unternehmen nach Artikel 33 DS-GVO: So meldete ein Unternehmen, dass es die Identität einer am Coronavirus erkrankten Beschäftigten allen weiteren im Unternehmen tätigen Beschäftigten bekannt gegeben hatte. Zweck war es, Kontaktpersonen der Erkrankten im Unternehmen über eine mögliche Infektion aufzuklären. Diese Vorgehensweise ist aus datenschutzrechtlicher Sicht jedoch nicht erforderlich. Vielmehr hätte die erkrankte Beschäftigte in diesem Fall nach ihren Kontakten im Unternehmen befragt werden können. Im Anschluss daran hätten die Kontaktpersonen – auch ohne eine Namensnennung der Erkrankten – über den Kontakt zu einer erkrankten Person informiert werden können. Ich verwarnte in diesem Fall das Unternehmen gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO.

J.2. Polizei und Verfassungsschutz

2.1 Polizei 2020 – Risiken sehen, Chancen nutzen!

Mit dem von der Innenministerkonferenz beschlossenen Programm Polizei 2020 könnten bisherige datenschutzrechtliche Defizite in der Informationsarchitektur der Polizei in Deutschland beseitigt und nachhaltige Verbesserungen erzielt werden. Dabei müssen allerdings an datenschutzrechtliche Kernforderungen berücksichtigt und die Datenschutzaufsicht eingebunden werden.

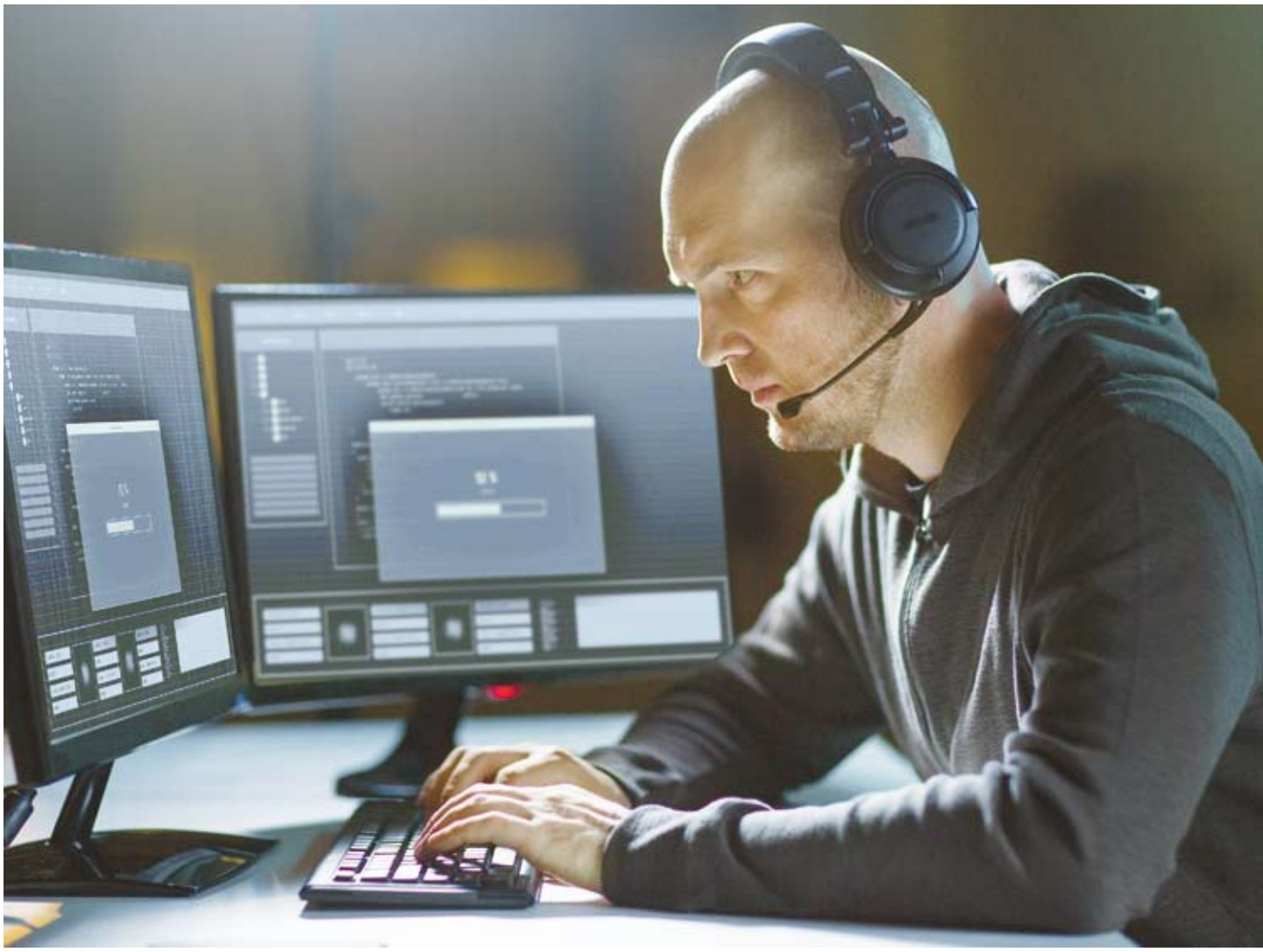
Bislang basiert die Informationsarchitektur der Polizei in Deutschland auf einer Vielzahl unterschiedlicher Datentöpfe, die kaum miteinander verbunden sind. Eine zersplitterte IT-Landschaft die von Eigenentwicklungen, Sonderlösungen, Schnittstellen, unterschiedlichen Dateiformaten und Erhebungsregeln geprägt ist, genügt nicht mehr den Anforderungen an die moderne Polizeiarbeit. Mit dem Programm Polizei 2020 soll ab dem Jahr 2025 eine gemeinsame, moderne und einheitliche Informationsarchitektur für die deutschen Polizeien in Bund und Ländern geschaffen werden. Im Ergebnis sollen die Polizistinnen und Polizisten jederzeit und überall Zugriff auf die Informationen haben, die sie benötigen, um ihre Aufgaben zu erfüllen. Ein weiteres Ziel ist es, die Polizeien von Bund und Ländern mit ihren nationalen und internationalen Partnern digital und medienbruchfrei zu vernetzen. Dabei müssen die rechtlichen Rahmenbedingungen und vor allem der Datenschutz berücksichtigt werden.

Polizeibeamte sollen überall auf notwendige Daten zugreifen können

Kernforderungen der Aufsichtsbehörden

Die Polizeibehörden in Bund und Ländern haben im Berichtsjahr einen ersten „fachlichen Bebauungsplan" für das Programm Polizei 2020 vorgelegt. Dieser benennt den Datenschutz als eines der Kernziele. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) begrüßte dies, monierte jedoch das Fehlen von ausreichenden Vorschlägen, wie das Projekt den Datenschutz stärken will. Die Konferenz forderte deshalb in einer Entschließung vom 16. April 2020, die Ziele und Meilensteine des Programms auch an datenschutzrechtlichen Kernforderungen auszurichten und die Datenschutzaufsicht in diesen Prozess einzubinden.

DSK-Entschließung Polizei 2020: https://t1p.de/Polizei2020



Aus Sicht der Datenschutzbehörden muss sich das Programm Polizei 2020 vorrangig auf die folgenden Ziele ausrichten:

1. Umfassende Bestandsaufnahme
   Eine Projektanalyse umfasst bislang nur Fragen der technischen Machbarkeit. Die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der vergangenen Jahre wurden nicht einbezogen. Dies ist in einer unabhängigen Evaluierung nachzuholen.

2. Rechtliche Leitplanken
   Mit dem neuen „Datenhaus“ in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende computergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und müssen deshalb gesetzlich und technisch begrenzt werden. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht. Die verantwortlichen Stellen müssen die gesetzlich und verfassungsrechtlich implizierten roten Linien bestimmen. Dies ist zwingend erforderlich, bevor Haushaltsmittel in großem Umfang eingesetzt werden.

Generalklauseln reichen nicht aus

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

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

Vorhandene Datenbestände bereinigen

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

Ich werde den weiteren Fortlauf des Programms intensiv begleiten, um den Datenschutz gemeinsam mit der Polizei nachhaltig zu verbessern. Meinerseits ist eine Konzentration auf die Beratung der Teilprojekte vorgesehen, in denen die Polizei Niedersachsen die (Co-) Federführung innerhalb der Programms Polizei 2020 übernommen hat. Diese Teilprojekte sind:

- „Kinderpornografie“: Durch künstliche Intelligenz unterstützte Erkennung kinderpornografischen Bild-/ und Videomaterials.

- „Wiederholungsprognose-Assistent“: Unterstützende Formulierungshilfe einer gerichtlich nachprüfbaren Wiederholungsprognose.

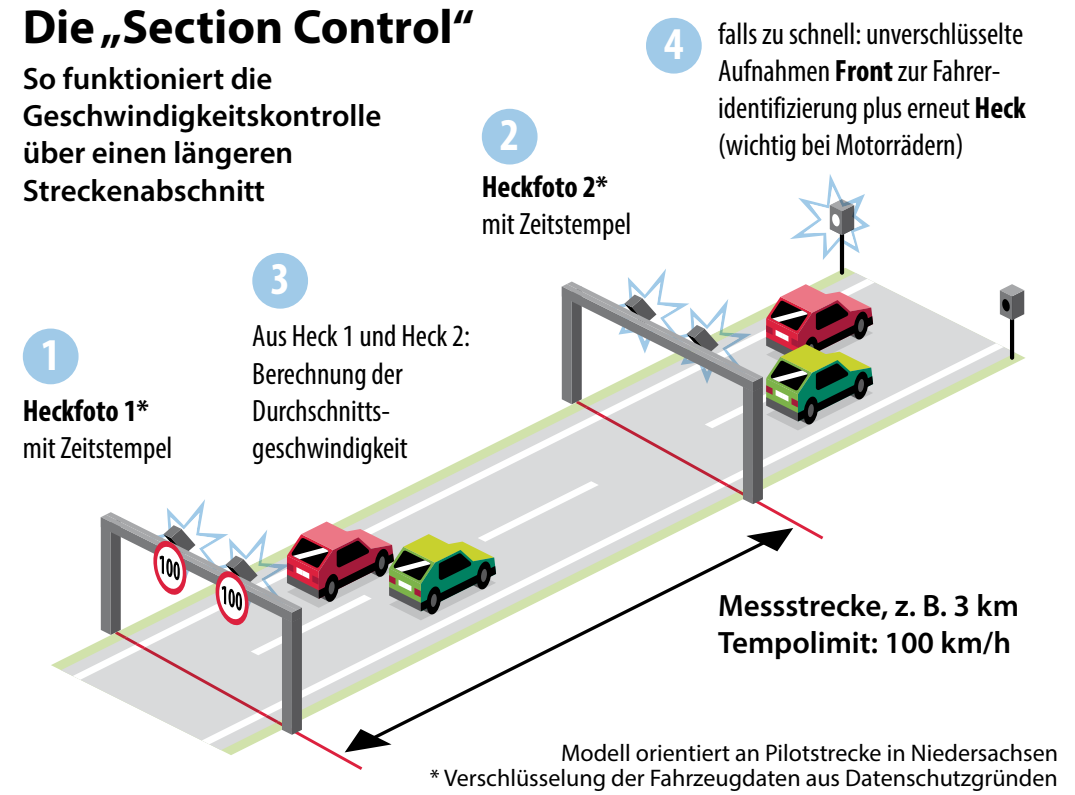
- „Mobilität“: Aufbau eines Kernteams und Bündelung von Wissen zur Entwicklung zukunftsweisender Applikationen.

2.2 Section Control: Der Weg durch alle Instanzen

In meinem 25. Tätigkeitsbericht hatte ich bereits über die „Section Control" genannte Anlage zur Abschnittskontrolle auf der Bundesstraße B 6 berichtet. Mit der Entscheidung des Bundesverwaltungsgerichts ist der seit 2019 laufende verwaltungsgerichtliche Rechtsstreit abgeschlossen. Das Gericht wies den Antrag des Klägers auf Zulassung der Revision zurück. Zudem wurde die im Oktober 2020 eingelegte Verfassungsbeschwerde nicht vom Bundesverfassungsgericht zur Entscheidung angenommen.

Funktion der „Section Control"

Die abschnittsbezogene Geschwindigkeitskontrolle „Section Control" ist ein Projekt des Niedersächsischen Ministeriums für Inneres und Sport zur Verkehrsüberwachung. Die Anlage zeichnet sich dadurch aus, dass sowohl bei der Ein- als auch bei der Ausfahrt des überwachten Streckenabschnitts je ein verschlüsseltes, mit Zeitstempel versehenes Heckfoto des passierenden Fahrzeugs gefertigt wird. Anhand eines Abgleichs dieser beiden mit Zeitstempel versehenen Fotos wird bei der Ausfahrt aus dem überwachten Bereich die Durchschnittsgeschwindigkeit ermittelt. Bei einer Überschreitung der zulässigen Höchstgeschwindigkeit wird eine unverschlüsselte Aufnahme der Front zur Fahreridentifizierung sowie des Hecks gefertigt. Wird die zulässige Höchstgeschwindigkeit dagegen nicht überschritten, werden die erfassten Datensätze automatisch gelöscht. Im Januar 2019 wurde die Anlage zunächst als Pilotprojekt in Betrieb genommen.



Mit seinem Beschluss vom 18. Dezember 2018[1] zur automatisierten Kraftfahrzeugkennzeichenkontrolle hatte das Bundesverfassungsgericht (BVerfG) festgestellt, dass auch bei sogenannten „Nichttrefferfällen" ein Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Person vorliegt. Vor diesem Hintergrund und in Ermangelung einer für die Kennzeichenerfassung erforderlichen Rechtsgrundlage forderte ich das Niedersächsische Innenministerium auf, das Pilotprojekt „Section Control" unverzüglich einzustellen. Denn nun wurde die Erfassung aller Fahrzeuge, die die Messstrecke passieren, als Eingriff in die informationelle Selbstbestimmung bewertet, und nicht mehr nur die Erfassung derjenigen, die zu schnell gefahren waren. Gleichermaßen äußerte ich mich in einer Anhörung des Innenausschusses im Februar 2019. Auf den Eilantrag eines betroffenen Bürgers hatte das Verwaltungsgericht (VG) Hannover den Betrieb der Anlage durch die Polizeidirektion Hannover vorläufig untersagt. Diese Entscheidung im einstweiligen Rechtsschutzverfahren wurde vom Oberverwaltungsgericht (OVG) Lüneburg zunächst bestätigt. Auch im Klageverfahren verwies das VG auf die fehlende Rechtsgrundlage und gab der Unterlassungsklage statt. Ich nahm als Beigeladene an den Verfahren teil.

Auch Nichttreffer sind ein Grundrechtseingriff

Mit Inkrafttreten des aktuellen § 32 Absatz 6 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) im Mai 2019 liegt nun die erforderliche gesetzliche Rechtsgrundlage für die automatisierte Kennzeichenerfassung vor. Auch nach Ansicht des OVG Lüneburg liegt damit eine ausreichende gesetzliche Eingriffsermächtigung für den Betrieb der Abschnittskontrolle auf der B 6 vor. Deshalb entsprach das OVG dem Antrag der Polizeidirektion Hannover im einstweiligen Rechtsschutzverfahren auf Änderung des Beschlusses. Ebenso änderte es im Hauptsacheverfahren die Entscheidung des VG Hannover im Sinne der Polizeidirektion. Gegen diese Entscheidung ließ das OVG Lüneburg keine Revision zu. Der betroffene Bürger legte daraufhin Nichtzulassungsbeschwerde vor dem Bundesverwaltungsgericht (BVerwG) ein.

NPOG schafft Rechtsgrundlage

Entscheidung des Bundesverwaltungsgerichts

Der Rechtsstreit wurde mit der Entscheidung des BVerwG verwaltungsgerichtlich abgeschlossen. Das BVerwG wies den Antrag des Klägers gegen die Nichtzulassung der Revision zurück. Das Urteil des OVG Lüneburg, wonach die Abschnittskontrolle rechtmäßig ist, wurde damit rechtskräftig.

Im Rahmen der Entscheidung über die Nichtzulassungsbeschwerde prüfte das BVerwG, ob

- die Rechtssache grundsätzliche Bedeutung hat,
- die Fortbildung des Rechts oder
- die Sicherung einer einheitlichen Rechtsprechung eine Revision erfordert oder
- ein Verfahrensmangel geltend gemacht wurde, auf dem die Entscheidung beruhen kann.

Nach Auffassung des BVerwG kam der Rechtssache keine grundsätzliche Bedeutung zu. Entgegen der Ansicht des Klägers bestehe eine Gesetzgebungskompetenz des Landes für die Einführung der „Abschnittskontrolle". Auch der Umstand, dass zur neuen Rechtsgrundlage im NPOG sowie zur Kenntlichmachung der „Abschnittskontrolle" keine höchstrichterliche Rechtsprechung existiere, begründe keine grundsätzliche Bedeutung der Rechtssache. Es bedürfe keiner höchstrichterlichen Klärung, wie eine landesrechtliche Norm auszulegen sei, da es sich hierbei nicht um reversibles Recht handele.

BVerwG sieht keine grundsätzliche Bedeutung

1 1 BvR 142/15

Die Voraussetzungen für eine Revisionszulassung wegen Abweichung des angegriffenen Urteils von der „höheren" Rechtsprechung waren nach Auffassung des BVerwG ebenfalls nicht erfüllt. Der Kläger sei seinen Darlegungserfordernissen nicht nachgekommen und habe keinen rechtlichen Obersatz herausgearbeitet, der von den vom Kläger angeführten Rechtssätzen aus der Rechtsprechung des Bundesverfassungsgerichts abweiche.

Aus der Beschwerde ließe sich zudem kein Verfahrensmangel entnehmen, auf dem die Entscheidung des Berufungsgerichts beruhe. Zum einen fehle es an einer Konkretisierung, welche Verfahrensvorschrift das Berufungsgericht in seiner Entscheidung verletzt haben soll. Zum anderen sei das Berufungsgericht seiner Pflicht zur Sachverhaltsaufklärung und Beweiserhebung nachgekommen und habe dem Kläger rechtliches Gehör nach Artikel 103 Absatz 1 des Grundgesetzes gewährt.

Verfassungsbeschwerde nicht angenommen

Der betroffene Kläger erhob daraufhin Verfassungsbeschwerde unter anderem wegen der Verletzung seines Grundrechts auf informationelle Selbstbestimmung. Neue wesentliche Gesichtspunkte wurden jedoch nicht vorgetragen. Der Beschwerdeführer beklagte insbesondere die formelle und materielle Verfassungswidrigkeit der Ermächtigungsnorm (keine Gesetzgebungskompetenz beim Land, Verstoß gegen den Verhältnismäßigkeitsgrundsatz) sowie die mangelhafte Kennzeichnung der Anlage. Das BVerfG nahm die Verfassungsbeschwerde nicht zur Entscheidung an. Auch wurde von einer Begründung abgesehen.

Keine Bedenken gegenüber Abschnittskontrolle

Da mit Inkrafttreten der neuen gesetzlichen Regelung die von mir geforderte bereichsspezifische Rechtsgrundlage für einen dauerhaften Betrieb der Abschnittskontrolle vorliegt und diese zudem aus meiner Sicht rechtskonform beschlossen wurde, erhebe ich keine datenschutzrechtlichen Bedenken mehr gegen die Abschnittskontrolle. Auch die datenschutzrechtlichen Transparenz- und Informationspflichten beim Betrieb der Anlage sind von der Polizeidirektion Hannover nach meiner Aufforderung erfüllt worden. Auf der Internetseite der Polizeidirektion finden sich die entsprechenden Angaben, sodass die Betroffenenrechte ausreichend gesichert sind.

Transparenzpflichten werden erfüllt

2.3 Fortsetzung der Prüfungen zur Videoüberwachung in Fußballstadien

Gemäß den „Richtlinien zur Verbesserung der Sicherheit bei Bundesspielen" des Deutschen Fußballbundes sind in den Stadien der Bundesliga, der 2. Bundesliga und der 3. Liga Videoüberwachungsanlagen zum Schutz der Besucherinnen und Besucher einzurichten. Auf Grund der hohen Anzahl an potenziell Betroffenen überprüfe ich weiterhin die entsprechenden Anlagen in Niedersachsen.

Tätigkeitsbericht 2019: https://t1p.de/TB2019

Nach einer im Herbst 2019 durchgeführten unangekündigten Vor-Ort-Prüfung der Videobeobachtung in einem Stadion konnte das Verfahren auch 2020 noch nicht vollständig abgeschlossen worden. Ein ebenfalls im Jahr 2019 zwischen der Polizei und der Betreibergesellschaft geschlossener (aktualisierter) Nutzungsvertrag über die installierte Videoüberwachungsanlage sah weiterhin Zutrittsrechte für Personen der Betreibergesellschaft und der Feuerwehr in einen besonders gesicherten Serverraum vor.

Auf den Servern befinden sich die (Video-)Aufnahmen der Polizei, die an Spieltagen beziehungsweise bei besonderen Großveranstaltungen auf Grundlage des § 32 Absatz 3 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) aufgezeichnet werden. Im Hinblick auf die sensiblen Aufnahmen, die auf dem Server vorgehalten werden, reichten mir die Festlegungen zu einem möglichen Zutritt und die entsprechende Dokumentation solcher Zutritte durch Dritte nicht aus. Aus diesem Grund habe ich die Polizei als Verantwortlichen für die erstellten Videoaufnahmen aufgefordert, in einer – mir noch vorzulegenden – (endgültigen) Datenschutz-Folgenabschätzung (DSFA) technisch-organisatorische Regelungen aufzunehmen, die für einen ausreichenden Schutz der polizeilichen Videoaufnahmen im Rahmen von erforderlichen Zutritten Dritter Sorge tragen.

Polizeiliche Aufnahmen müssen ausreichend geschützt werden

Einigung zwischen Polizei und Betreiber absehbar

Mittlerweile scheint sich abzuzeichnen, dass eine datenschutzrechtlich vertretbare Einigung zwischen der Polizei und dem Betreiber bezüglich der Zutrittsregelungen und deren Dokumentation beziehungsweise der Nachvollziehbarkeit erzielt werden konnte. Ich gehe deshalb davon aus, die endgültige DSFA durch die Polizei noch im Frühjahr 2021 zu erhalten.

Zudem führte die bei meiner Kontrolle im Herbst 2019 festgestellte unrechtmäßige Verarbeitung von personenbezogenen Daten in diesem Stadion zwischenzeitlich zur Einleitung eines Bußgeldverfahren gegen den Betreiber. Zu bemängeln war dabei insbesondere die Speicherung anlassloser Videoaufnahmen über einen Zeitraum von vier Wochen (statt der zulässigen 72 Stunden).

Bußgeldverfahren wegen langer Speicherung

Ausblick

Von den im 25. Tätigkeitsbericht angekündigten Prüfungen in zwei weiteren Fußballstadien habe ich 2020 aus Gründen des Gesundheitsschutzes im Rahmen der Pandemiebekämpfung Abstand genommen. Ich hoffe, diese Prüfungen im Jahr 2021 abschließen zu können.

2.4 Rechtswidrige Datenverarbeitung durch den Niedersächsischen Verfassungsschutz

Mit Schreiben vom 15. Juni 2020 teilte mir der Präsident des Niedersächsischen Verfassungsschutzes mit, dass es in „seiner Behörde zu einer rechtswidrigen Verarbeitung personenbezogener Daten" gekommen sei. Durch eine Verwechselung war die falsche Person von einer nachrichtendienstlichen Maßnahme betroffen.

Präsident ordnet Überprüfung der Abläufe an

Gemäß den zitierten Angaben des Verfassungsschutzpräsidenten gegenüber der Presse am selben Tag sei es in der Sachbearbeitung des konkreten Falles zu Fehlern gekommen. Daher habe er, um weitere Fälle ausschließen zu können, eine Überprüfung der vorgeschriebenen Arbeitsabläufe im betroffenen Fachbereich sowie in allen Arbeitsbereichen angeordnet.

Der Niedersächsische Verfassungsschutz unterliegt nicht den Bestimmungen der sogenannten Richtlinie für Justiz und Inneres (JI-Richtlinie) beziehungsweise jenen des – die JI-Richtlinie umsetzenden – zweiten Teils des Niedersächsischen Datenschutzgesetzes (NDSG). Stattdessen sind gemäß § 2 Nummer 2 Buchstabe c NDSG grundsätzlich die Regelungen der Datenschutz-Grundverordnung (DS-GVO) auf die Verarbeitungen von personenbezogenen Daten durch den Niedersächsischen Verfassungsschutz anzuwenden.

Verarbeitung ohne Rechtsgrundlage

Im vorliegenden Fall überprüfte ich den Niedersächsischen Verfassungsschutz im Rahmen meiner gesetzlichen Befugnisse. Dabei stellte ich fest, dass ein Verstoß gegen den in Artikel 5 Absatz 1 Buchstabe a in Verbindung mit Artikel 6 Absatz 1 DS-GVO normierten „Grundsatz der Rechtmäßigkeit" vorlag. Die Verarbeitung der personenbezogenen Daten hatte in diesem Fall ohne eine Rechtsgrundlage stattgefunden. Durch eine (Identitäts-)Verwechselung war die falsche Person von der nachrichtendienstlichen Maßnahme betroffen. Somit wurden die Daten einer Person verarbeitet, ohne dass diese dazu Anlass gegeben hatte, überwacht zu werden.

Verfassungsschutz wird verwarnt

Kurz nach Ende des Berichtszeitraums schloss ich das Verfahren mit einer Verwarnung gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO ab. Von der Darlegung weiterer Einzelheiten muss ich aus Gründen des Geheimschutzes absehen.

2.5 Beanstandung des Polizei-Messengers NIMes

Der eigens für die Niedersächsische Polizei eingeführte Niedersachsen-Messenger (NIMes) wird mittlerweile flächendeckend durch mehr als 21.000 Beamtinnen und Beamte genutzt. In meinem 24. und 25. Tätigkeitsbericht habe ich meine grundlegenden Bedenken aus datenschutzrechtlicher Sicht bereits dargestellt. Inzwischen habe ich NIMes offiziell beanstandet.

Am 4. Juni 2020 wurde mir durch das Niedersächsische Ministerium für Inneres und Sport eine Datenschutz-Folgenabschätzung (DSFA) vorgelegt. Ich prüfte diese zunächst unter dem Aspekt der Nutzung privater Endgeräte und der hierzu umgesetzten technisch-organisatorischen Schutzmaßnahmen zur Verringerung von Sicherheitslücken. Meine Prüfung ergab, dass die ergriffenen technischen Schutzmaßnahmen nicht ausreichend sind. Ich forderte unter anderem, ein sogenanntes Mobile Device Management (MDM) einzuführen, welches dem Verantwortlichen die Möglichkeit eröffnet, die volle Kontrolle über den Messenger auch auf privaten Endgeräten auszuüben. Als weitere Option schlug ich erneut vor, diese sensible Anwendung ausschließlich auf dienstlichen Endgeräten auszuführen, die entsprechend technisch gesichert werden.

Bereits in diesem Teilaspekt meiner Prüfung stellte ich große technische und organisatorische Defizite fest. Insbesondere die Kombination aus einer hohen Schutzwürdigkeit der verarbeiteten Daten (bis einschließlich Schutzstufe D meines Schutzstufenkonzeptes) und der Gefahr, dass polizeiliche IT-Anwendungen häufig ein begehrtes Ziel für Angreifer darstellen, führt zu einem inakzeptablen Risiko für die mit NIMes verarbeiteten personenbezogenen Daten von Bürgerinnen und Bürgern sowie Polizistinnen und Polizisten. Stufe D des Schutzstufenkonzepts umfasst Daten, deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte. Durch den Einsatz privater Endgeräte ist im laufenden Betrieb eine unüberschaubare Kombination von verschiedenen Geräten, Betriebssystemen, sonstiger Software und Konfigurationen im Einsatz. Gleichzeitig ist der jeweilige Anwender oder die Anwenderin dafür verantwortlich, das private Endgerät vor Schadprogrammen zu schützen. Das wird dem Schutzbedarf der bedrohten Daten in keiner Weise gerecht.

Schutzstufenkonzept: https://t1p.de/Schutzstufenkonzept

Ich habe daher kurz nach Ende des Berichtszeitraums die Anwendung gemäß § 57 Absatz 5 des Niedersächsischen Datenschutzgesetzes (NDSG) gegenüber dem Ministerium für Inneres und Sport beanstandet.

Abschluss des Verfahrens – Beanstandung und sonst nichts?

Pressemitteilung zur Beanstandung: https://t1p.de/pm-nimes

Durch diese Beanstandung, auf die noch eine Stellungnahme des Niedersächsischen Innenministeriums folgt, ist meine datenschutzrechtliche Prüfung abgeschlossen. Weitergehende Abhilfebefugnisse wie etwa die Anweisung, die personenbezogenen Daten in NIMes datenschutzkonform zu verarbeiten, eine Beschränkung oder ein Verbot der Datenverarbeitung, kann ich leider mangels entsprechender Regelungen im NDSG oder im Fachrecht nicht ausüben. Der niedersächsische Gesetzgeber hat es bisher europarechtswidrig versäumt, die entsprechenden Regelungen des Artikels 47 der JI-Richtlinie umzusetzen. Meine Forderung nach vollständiger Umsetzung der JI-Richtlinie bleibt nach wie vor bestehen.

J.3. Justiz

3.1 Aufsichtsbefugnis gegenüber Gerichten – Auslegung der justiziellen Tätigkeit

Nach dem rechtsstaatlichen Grundsatz der Gewaltenteilung wird die Staatsgewalt durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt.[1] Damit einher geht der Grundsatz der richterlichen Unabhängigkeit. Danach sind die Richterinnen und Richter sachlich und persönlich unabhängig und nur an das Recht gebunden.[2] Doch wie sind diese verfassungsrechtlichen Grundsätze in der datenschutzrechtlichen Aufsicht ausgestaltet?

Die Aufsichtsbefugnis meiner Behörde gegenüber den Gerichten ist in Artikel 55 Absatz 3 der Datenschutz-Grundverordnung (DS-GVO) geregelt. Danach ist die Aufsichtsbehörde nicht zuständig für die Aufsicht über die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen. Um die gerichtliche Unabhängigkeit zu wahren, besteht keine Kontrollbefugnis der Aufsichtsbehörden, soweit das gerichtliche Handeln als justizielle Tätigkeit einzustufen ist. Gleiches gilt für den Bereich der Strafverfolgung und Gefahrenabwehr nach Artikel 45 Absatz 2 der JI-Richtlinie, der in § 55 Absatz 1 Satz 2 und § 57 Absatz 3 Satz 2 des Niedersächsischen Datenschutzgesetzes (NDSG) umgesetzt wurde. Das Gegenstück zur justiziellen Tätigkeit bildet die Wahrnehmung von Verwaltungsaufgaben.[3]

Keine Kontrolle richterlichen Handelns

Auslegung der LfD Niedersachsen

Den Begriff der justiziellen Tätigkeit lege ich restriktiv aus. Erfasst wird nur die richterliche Tätigkeit als solche. Alle Verarbeitungen im Zusammenhang mit der gerichtlichen Entscheidungsfindung einschließlich deren Vorbereitung und Durchführung unterliegen grundsätzlich nicht der hiesigen Kontrolle.

1 Artikel 20 Absatz 2 Satz 2 des Grundgesetzes (GG)

2 Artikel 97 Absatz 1 GG; siehe auch Artikel 47 der Charta der Grundrechte der Europäischen Union

3 Siehe auch § 1 Absatz 2 NDSG

Aufsicht über Verwaltungsaufgaben möglich

Jedoch stellen Datenverarbeitungen an den Gerichten, denen keine richterliche Würdigung zugrunde liegt, Verwaltungsaufgaben dar, für die die Aufsicht durch meine Behörde eröffnet ist.

Bei der Auslegung des Begriffs der justiziellen Tätigkeit kann es mitunter zu Abgrenzungsschwierigkeiten kommen. Nach meiner Auffassung ist meine Aufsichtsbefugnis nicht per se bei jedem Handeln von Beschäftigten der Gerichte mit Bezug zu einem gerichtlichen Verfahren beschränkt. Vielmehr bedarf es einer genauen Differenzierung, wem der konkrete datenschutzrechtliche Verstoß zuzuordnen ist. Sofern beispielsweise der Geschäftsstelle bei Ausführung der richterlichen Verfügung ein Fehler unterläuft, zum Beispiel durch Fehladressierung einer Akte oder durch einen Kuvertierungsfehler, wird durch eine aufsichtsbehördliche Kontrolle die richterliche Unabhängigkeit nicht tangiert. Dem konkreten Fehlversand liegt ein individuelles menschliches Fehlverhalten der Geschäftsstelle zugrunde. Dieses stellt keine richterliche Würdigung dar, die einer Einflussnahme durch die Aufsichtsbehörde entzogen werden müsste. Die Versendung von Akten und anderen Schriftstücken im Rahmen des gerichtlichen Verfahrens ist ein reiner Verwaltungsvorgang, der von der richterlichen Entscheidungsfindung an sich zu unterscheiden ist. Auf die richterliche Entscheidung wird kein Einfluss genommen, wenn Verfahrensabläufe in technischer und/oder organisatorischer Hinsicht überprüft werden. Hierdurch erfolgt eine Sensibilisierung der Verantwortlichen für den Datenschutz sowie eine Stärkung des datenschutzrechtlichen Bewusstseins für künftige Verarbeitungsvorgänge. Organisationsabläufe können so optimiert werden.

Datenpannen müssen gemeldet werden

Im Rahmen meiner Zuständigkeit sind entsprechende Datenschutzverletzungen nach Artikel 33 DS-GVO beziehungsweise im Bereich der Strafverfolgung und Gefahrenabwehr nach § 41 NDSG zu melden. Zudem weise ich darauf hin, dass die Regelungen zur Benachrichtigung des Betroffenen nach Artikel 34 DS-GVO oder § 42 NDSG stets einzuhalten sind.

Auslegung des Justizministeriums

Das Niedersächsische Justizministerium (MJ) legt den Begriff der justiziellen Tätigkeit dagegen nicht derart restriktiv aus. Nach Auffassung des MJ müssen justizielle Tätigkeiten im Sinne des Artikel 55 Absatz 3 DS-GVO einen derart hinreichenden sachlich-funktionalen sowie personellen Bezug zur richterlichen Entscheidungsfindung aufweisen, dass sie im Interesse der richterlichen Unabhängigkeit von externer Kontrolle nicht beeinflusst werden sollen. Der sachlich-funktionelle Bezug erstrecke sich auf sämtliche datenverarbeitende Tätigkeiten, die im Rahmen der Rechtsprechung in einem konkreten gerichtlichen Verfahren vorgenommen würden. Der personelle Bezug umfasse sämtliche Personen, die im Zusammenhang mit einem konkreten gerichtlichen Verfahren der Organisations- und Einflusssphäre der Justiz zuzuordnen seien. Eine Meldung von Datenschutzverletzungen sei entsprechend nicht erforderlich, soweit die justizielle Tätigkeit betroffen sei.

Unterschiede bei der Auslegung und Ausblick

Im Wesentlichen haben das MJ und ich ein gleiches Verständnis zur Auslegung des Begriffs der justiziellen Tätigkeit. Die Auffassungen unterscheiden sich jedoch im Hinblick auf die Einstufung der Tätigkeit von Beschäftigten bei Gericht, zum Beispiel der Geschäftsstelle, als justizielle Tätigkeit. Während das MJ aufgrund des personellen Bezugs zur richterlichen Entscheidungsfindung eine Aufsichtsbefugnis der LfD verneint, kommt es nach meiner Auffassung auf die Zuordnung des datenschutzrechtlichen Verstoßes im konkreten Einzelfall an.

Konstruktive Gespräche, aber keine Einigung

Eine in Gänze übereinstimmende Rechtsansicht konnte bisher trotz eines konstruktiven Austausches mit dem MJ nicht gefunden werden. Eine endgültige Klärung wird daher wohl nur durch eine richterliche Entscheidung im Einzelfall herbeigeführt werden können.

3.2 Einrichtung besonderer Stellen im Justizsystem

Gemäß den europäischen Regelungen müssen die Gerichte die datenschutzrechtlichen Vorgaben in gleicher Weise beachten wie die übrigen öffentlichen Stellen. Auch bestehen hinsichtlich der Betroffenenrechte grundsätzlich keine Einschränkungen. Allerdings steht mir keine Aufsichtsbefugnis gegenüber den Gerichten zu, sofern diese im Rahmen der justiziellen Tätigkeit personenbezogene Daten verarbeiten. Es stellt sich die Frage, wie diese aufsichtsrechtliche Lücke geschlossen werden kann.

In der Datenschutz-Grundverordnung (DS-GVO) und der sogenannten JI-Richtlinie sind keine ausdrücklich verpflichtenden Regelungen enthalten, welche die Zuweisung der Zuständigkeit für die Aufsicht über Datenverarbeitungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit betreffen. Stattdessen sollen nach Erwägungsgrund 20 der DS-GVO „besondere Stellen im Justizsystem" des Mitgliedsstaates mit der Aufsicht betraut werden. Diese sollen insbesondere die Einhaltung der Vorschriften der Verordnung sicherstellen, Richterinnen, Richter und Staatsanwaltschaften besser für die Pflichten aus der Verordnung sensibilisieren und Beschwerden in Bezug auf Datenverarbeitungsvorgänge bearbeiten. Gleiches sieht der Erwägungsgrund 80 der JI-Richtlinie vor, wonach unter Verweis auf Artikel 8 Absatz 3 der Charta der Grundrechte der Europäischen Union eine „unabhängige Stelle" die Einhaltung des Schutzes personenbezogener Daten überwachen soll.

Sensibilisierung und Bearbeitung von Beschwerden

Umsetzung in Niedersachsen

Die vorgesehenen Aufsichtsstellen im Justizsystem wurden in Niedersachsen leider bislang nicht eingerichtet. Bei einem Treffen mit dem Niedersächsischen Justizministerium wiesen Beschäftigte meiner Behörde darauf hin, wie dringend die „besonderen Stellen im Justizsystem" geschaffen werden müssen. Das Niedersächsische Justizministerium kam meiner Bitte um Prüfung nach, das Ergebnis lag bis zum Jahresende 2020 noch nicht vor.

Prüfung des MJ noch nicht abgeschlossen

In jedem Fall ist es erforderlich, den „aufsichtslosen" Bereich der justiziellen Tätigkeit (siehe J.3.1, S. 135) im Rahmen der Auslegung so stark wie möglich einzugrenzen, um die Folgen dieser Lücke für die Betroffenen möglichst gering zu halten.

3.3 Aufsicht über Staatsanwaltschaften

Die Aufsichtsbefugnis meiner Behörde über Staatsanwaltschaften wird in § 57 Absatz 3 des Niedersächsischen Datenschutzgesetzes (NDSG) geregelt. Danach ist die Aufsicht über die Erhebung personenbezogener Daten durch Strafverfolgungsbehörden bei der Ermittlung, Aufdeckung oder Verfolgung von Straftaten erst nach Abschluss des Strafverfahrens zulässig. Zudem erstreckt sie sich nicht auf eine Datenverarbeitung, die gerichtlich überprüft wurde. Zwischen meiner Behörde und dem Niedersächsischen Justizministerium bestehen unterschiedliche Auffassungen darüber, wie diese Regelungen auszulegen sind.

§ 57 Absatz 3 NDSG setzt Artikel 45 Absatz 3 der sogenannten JI-Richtlinie in Verbindung mit Erwägungsgrund 80 der Richtlinie um, wonach „unabhängige Justizbehörden im Rahmen ihrer justiziellen Tätigkeit" ebenfalls wie Gerichte von der Aufsicht durch die Aufsichtsbehörden ausgenommen werden können. Als Beispiel für unabhängige Justizbehörden nennt EG 80 JI-Richtlinie ausdrücklich die Staatsanwaltschaften.
In der Gesetzesbegründung zu § 57 Absatz 3 NDSG heißt es, dass die Staatsanwaltschaften einbezogen seien, da die Frage der Verwertbarkeit von Daten im Strafverfahren den jeweils erkennenden Gerichten abschließend und ausschließlich übertragen bleibe. Da für diese abschließende Beurteilung die Gewährleistung einer bis zu diesem Zeitpunkt vollständigen und unveränderten Daten- und Aktenlage unabdingbar sei, könne sich die Kontrollbefugnis bis zum Abschluss des Strafverfahrens nicht auf die Strafverfolgungsbehörden erstrecken.

Ansicht der LfD Niedersachsen

Zunächst ist unter Hinweis auf das Urteil des Europäischen Gerichtshofs vom 27. Mai 2019[1] zweifelhaft, ob die Staatsanwaltschaften wegen des einzelfallbezogenen Weisungsrechts der Landesjustizministerien aus § 146 und 147 des Gerichtsverfassungsgesetzes als „unabhängige Justizbehörden" im Sinne der JI-Richtlinie angesehen werden können. Insofern würde die Regelung in § 57 Absatz 3 NDSG mit den europarechtlichen Vorgaben nicht im Einklang stehen.

Kontrolle auch während eines Verfahrens möglich

Ungeachtet dessen ergibt sich bereits aus den Motiven des Gesetzes, dass nicht per se jedes Handeln der Staatsanwaltschaft einer Aufsicht durch die Aufsichtsbehörden entzogen ist. Vielmehr ist eine Kontrollbefugnis – auch während eines laufenden Strafverfahrens – zu bejahen, soweit reine Verwaltungstätigkeiten betroffen sind. Die staatsanwaltschaftliche Tätigkeit soll lediglich in dem Umfang, in dem im späteren gerichtlichen Verfahren eine richterliche Würdigung im Rahmen der justiziellen Tätigkeit erfolgt, von der

1 Aktenzeichen C-508/18

Aufsicht der Aufsichtsbehörde ausgenommen sein. Sind dagegen keine justiziellen Tätigkeiten, sondern reine Verwaltungstätigkeiten betroffen (zum Beispiel bei Abhandenkommen einer Akte oder Aktenversendung an den falschen Adressaten durch die Geschäftsstelle), besteht eine Kontrollbefugnis durch die Aufsichtsbehörde.

Datenpannen sind in diesem Fall nach § 41 NDSG zu melden. Ergänzend weise ich darauf hin, dass – sofern keine richterliche Entscheidung über die Datenverarbeitung ergangen ist – nach Abschluss des Strafverfahrens in jeden Fall eine Datenpannenmeldung erfolgen muss. Zudem sind die Mitteilungspflichten an den Betroffenen nach § 42 NDSG zu beachten.

Ansicht des Justizminisierums

Das Niedersächsische Justizministerium (MJ) vertritt dagegen die Auffassung, dass die Aufsicht durch meine Behörde durch den niedersächsischen Gesetzgeber in § 57 Absatz 3 NDSG bis zum Abschluss des jeweiligen Verfahrens gänzlich ausgeschlossen worden sei. In Ermangelung eines Aufsichtsrechts bestehe für die Zeit des Ausschlusses des Aufsichtsrechts auch keine Pflicht zur Meldung von Datenpannen. Meine Auffassung, dass die Staatsanwaltschaften im Rahmen ihrer justiziellen Tätigkeit ebenso wie Gerichte von der Aufsicht durch die LfD ausgenommen seien, werde geteilt. Nach Auffassung des MJ stellen jedoch sämtliche im Rahmen der Bearbeitung der konkreten Einzelrechtssache veranlassten Entscheidungen und Verfügungen aufgrund des personellen Bezugs zur späteren richterlichen Entscheidungsfindung eine justizielle Tätigkeit dar. In der Konsequenz sei daher eine Aufsicht durch meine Behörde ausgeschlossen.

Unterschiede bei der Auslegung und Ausblick

Gerichtliche Klärung ist notwendig

Im Ergebnis stellt das MJ für die Bestimmung der Zuständigkeit primär auf die zeitliche Komponente ab. Darüber hinaus stuft das MJ sämtliche im Rahmen der Fallbearbeitung veranlassten Handlungen als justizielle Tätigkeit ein. Im Gegensatz dazu bin ich der Ansicht, dass nicht per se jedes Handeln der Staatsanwaltschaft als justizielle Tätigkeit eingestuft werden kann. Vielmehr bedarf es einer Prüfung im Einzelfall, ob der konkrete datenschutzrechtliche Verstoß der justiziellen Tätigkeit oder der Verwaltungstätigkeit zuzuordnen ist.
Trotz eines konstruktiven Austausches konnte zwischen den Behörden bislang keine in Gänze übereinstimmende Rechtsauffassung erreicht werden. Eine endgültige Entscheidung wird nur durch eine gerichtliche Klärung herbeigeführt werden können.

J.4. Kommunen und Landesverwaltung

4.1 Beschwerden gegen die Pflegekammer Niedersachsen

Zu Datenverarbeitung durch die Pflegekammer Niedersachsen erreichten mich zahlreiche Beschwerden im Zusammenhang mit dem Kammermagazin und einer Online-Befragung. Datenschutzverstöße lagen aber in beide Fällen nicht vor.

Zulässige Auftragsverarbeitung für den Versand des Kammermagazins

19 individuelle Beschwerden richteten sich gegen das Kammermagazin, das Mitteilungsblatt der Pflegekammer Niedersachsen. Die Beschwerdeführenden wendeten sich dagegen, dass in Zusammenhang mit Druck und Versand die personenbezogenen Daten der Mitglieder an eine Verlagsgesellschaft, gegeben werden. Meine Prüfung ergab, dass es sich hierbei um eine zulässige Auftragsverarbeitung handelt. Eine Auftragsverarbeitung liegt vor, wenn unter der Aufsicht des Auftraggebers Hilfstätigkeiten für diesen ausgeführt werden, aber die datenschutzrechtliche Verantwortung allein beim Auftraggeber verbleibt. Der Druck und Versand von Unterlagen ist hierfür ein typisches Beispiel. Die Verwendung von personenbezogenen Daten durch den Auftragnehmer ist keine Datenübermittlung im Rechtssinne. Vielmehr handelt es sich immer noch um eine Verarbeitung in der Verantwortung des Auftraggebers. Deshalb ist in diesen Konstellationen auch keine gesetzliche Übermittlungsregelung erforderlich.

Um allerdings die vielfältigen datenschutzrechtlichen Pflichten des Auftraggebers in solchen Konstellationen abzusichern, ist ein Auftragsverarbeitungsvertrag notwendig. Artikel 28 der Datenschutz-Grundverordnung (DS-GVO) legt detailliert fest, welche Pflichten der Auftraggeber dem Auftragnehmer hierbei übertragen muss. Bei der Prüfung des Vertrags zwischen Pflegekammer und Verlagsgesellschaft stellte ich fest, dass alle Anforderungen erfüllt waren. Auch die übrige Zuarbeit der Verlagsgesellschaft verlief im Rahmen

der Auftragsverarbeitung. Ein Datenschutzverstoß lag nicht vor. Dies habe ich den Beschwerdeführenden mitgeteilt.

Beschwerden zu Online-Befragung

Sieben weitere Beschwerden richteten sich gegen das Niedersächsische Ministerium für Soziales, Gesundheit und Gleichstellung im Zusammenhang mit einer freiwilligen Online-Befragung der Mitglieder zur Evaluation der Pflegekammer.
Die Beschwerdeführenden äußerten den Verdacht auf unerlaubte Zugriffe bzw. Manipulationsversuche durch Dritte in Zusammenhang mit der Befragung. Meine Prüfung ergab, dass weder ein Hackerangriff noch ein Datenleck, durch das personenbezogene Daten in die Hände Dritter gelangen könnten, stattgefunden hatte. Allerdings war es aufgrund eines technischen Fehlers in der Befragungssoftware möglich, den Link zum Fragebogen weiterzugeben. Ein solcher Link konnte beispielsweise aus sozialen Netzwerken heraus durch Dritte geöffnet werden. Es kam in 59 Fällen zu einer Einsichtnahme durch Dritte in ausgefüllte Fragebögen. Im Rahmen meiner Prüfung stellte ich fest, dass selbst bei dieser Einsichtnahme keine Verletzung des Schutzes personenbezogener Daten stattgefunden hatte. Dies zum einen deshalb, weil kein Einblick in die IP-Adressen der Berechtigten möglich war. Zum anderen ließ auch der ausgefüllte Fragebogen aufgrund der Vielzahl an Teilnehmenden keinen Rückschluss auf die Identität der Berechtigten zu.

Kein Datenschutzverstoß bei der Online-Befragung

Konkret hatten zum Zeitpunkt der Manipulationsvorwürfe ca. 7000 Mitglieder an der Befragung teilgenommen, die Gesamtzahl der Teilnahmeberechtigten betrug 80.000 Mitglieder. Selbst unter Berücksichtigung der Abfrage der ersten beiden Ziffern der Wohnort-Postleitzahl war kein Rückschluss auf die Identität einzelner Personen möglich, da diese sogenannten Leitregionen einen sehr großen Einzugsbereich haben. Daher war auch in Kombination mit den abstrakt abgefragten Kategorien insbesondere zum eigenen Berufsabschluss keine Rückschlussmöglichkeit auf einzelne Personen gegeben. Eine Einsichtnahme durch Dritte in ausgefüllte Fragebögen hatte daher keinen Bezug zu personenbezogenen Daten und es lag in keinem Fall eine Datenschutzverletzung vor.

Gesetz zur Auflösung der Pflegekammer

Im Oktober 2020 übersandte mir das Sozialministerium den Gesetzentwurf zur Auflösung der Pflegekammer mit Gelegenheit zur Stellungnahme. Der Entwurf regelt die Abwicklung der Pflegekammer, insbesondere hinsichtlich der Erfüllung von Verbindlichkeiten und Verpflichtungen sowie der Rückzahlung von Mitgliedsbeiträgen. § 5 des Gesetzesentwurfs sieht eine Befugnis des Landes zur Verarbeitung der Daten der Kammermitglieder für die Abwicklung der Pflegekammer vor. Zudem ist es ausdrücklich vorgesehen, die Daten der Kammermitglieder zu löschen, sobald diese nicht mehr für die Abwicklung erforderlich sind, frühestens drei Jahre nach Auflösung der Kammer. Diese Löschfrist entspricht der üblichen Verjährungsfrist. Vor dem Hintergrund der stets möglichen Geltendmachung von Forderungen gegen die Kammer ist diese geplante Gesetzesregelung nachvollziehbar. Gegen den vorgelegten Entwurf bestehen daher keine datenschutzrechtlichen Bedenken.

Keine Bedenken gegen den Gesetzesentwurf

4.2 Gesetzesgrundlage für digitale Wasserzähler fehlt

In etlichen Wasserverbänden dürfte sich bei zukünftigen Investitionen die Frage stellen, ob die analogen Wasserzähler durch digitale (mit oder ohne Funkmodul) ersetzt werden sollten. Digitale Wasserzähler sind allerdings in der Lage, personenbezogene Daten in einem Umfang zu verarbeiten, der eine ausdrückliche Rechtsgrundlage erfordert. Eine Ermächtigungsgrundlage im Landesrecht ist jedoch bislang nicht in Sicht. Die Rechtsunsicherheit in Niedersachsen ist daher groß.

Bei der öffentlichen Trinkwasserversorgung unterliegen die Haushalte dem sogenannten Anschluss- und Benutzungszwang. Die Verbraucherinnen und Verbraucher können sich den Wasserversorger nicht aussuchen. Aufgrund dieses Pflichtverhältnisses haben sie grundsätzlich kein Wahlrecht, welche Auslesetechnik in ihrem Haushalt installiert wird. Insbesondere bei Einfamilienhäusern und Häusern mit zwei Wohneinheiten (sofern dem Wasserversorger die Verbrauchsmenge der anderen Einheit bekannt ist) wäre ein Rückschluss auf das Verbrauchsverhalten eines konkreten Haushalts möglich. Somit würde es sich um personenbezogene Daten handeln, für deren Verarbeitung eine Rechtsgrundlage erforderlich ist.

Die Ablesung der gegenwärtigen analogen Wasserzähler beruht auf der Verordnung über Allgemeine Bedingungen für die Versorgung mit Wasser (AVBWasserV).[1] Gemäß § 24 Abs. 1 AVBWasserV erfolgt die Abrechnung entweder pro Monat oder in größeren Zeitabschnitten, die zwölf Monate nicht wesentlich überschreiten dürfen. Gemäß §§ 1 Abs. 1; 35 Abs. 1 AVBWasserV sind die Regelungen der AVBWasserV sowohl bei privatrechtlicher Ausgestaltung des Benutzungsverhältnisses (in den Versorgungsverträgen bzw. Vertragsbedingungen) als auch bei öffentlich-rechtlicher Ausgestaltung (in den Gebührensatzungen) umzusetzen. Aus den §§ 20, 24 Abs. 1 AVBWasserV ergibt sich zugleich die gegenwärtige Ablesetaktung, die allenfalls monatlich erforderlich ist.

Was bedeutet das für zukünftige digitale Wasserzähler?

Bisherige Rechtsgrundlage genügt nicht

Selbst wenn ein digitaler Wasserzähler per Funk nur dieselbe Verbrauchsinformation und Ablesetaktung abbilden würde wie ein bisheriger analoger Wasserzähler, könnte die damit verbundene Datenverarbeitung nicht auf die genannten Regelungen gestützt werden. Dies beruht darauf, dass § 20 AVBWasserV nur für die dort genannte Art und Weise der Ablesung (in den Räumen des Verbrauchers bzw. der Verbraucherin durch das Wasserversorgungsunternehmen bzw. durch Selbstablesung) eine Rechtsgrundlage darstellt.

1 Bisherige Rechtsgrundlage für die Ablesung der (analogen) Wasseruhr beim Verbraucher / der Verbraucherin sind §§ 18 Abs. 1, 20, 24 AVBWasserV (vgl. auch die Auskunftspflicht der §§ 26 Abs. 1 – 3; 4 Wasserverbandsgesetz).

Ein digitaler Wasserzähler, der das Ablesen per Funk ermöglicht, kann auf die allgemeine Aufgabennorm des § 3 Abs. 1 Niedersächsisches Datenschutzgesetz (NDSG) gestützt werden, wenn sich die Verarbeitung im Rahmen der bisherigen Erforderlichkeit hält. Das setzt voraus, dass – wie bislang – nur der aktuelle Verbrauchswert ausgelesen werden kann. Zudem muss die bisherige maximal monatliche Ablesemöglichkeit eingehalten werden. Im Fall eines Auszugs oder Einzugs ist zudem eine anlassbezogene Ablesung möglich. Mit dieser Ablesemöglichkeit bewegt sich ein digitaler Funkwasserzähler im Rahmen der Erforderlichkeit gemäß § 3 Abs. 1 NDSG, wie sie gegenwärtig durch die AVBWasserV vorgegeben ist. Daneben wird eine Ablesung in maximal monatlicher Taktung mit Funkzähler auch auf eine wirksame Einwilligung der Betroffenen gegenüber dem Wasserversorger gestützt werden können.

Grundrechtseingriff ohne Rechtsgrundlage

Sofern zukünftige digitale Funkwasserzähler eine höhere Auslesetaktung ermöglichen – entweder mit oder ohne Funk – bzw. weitere Verbrauchsdaten speichern (z.B. Verbrauchshistorie; Höchstdurchfluss; Umgebungstemperatur), wäre eine solche Datenverarbeitung weder von der AVBWasserV noch von § 3 Abs. 1 NDSG gedeckt. Die Installation eines digitalen Wasserzählers, der eine Vielzahl an Verbrauchswerten „mit Zeitstempel" speichert, würde die Erstellung von Persönlichkeits- und Verhaltensprofilen der Betroffenen durch öffentliche Stellen ermöglichen. Es würde sich um einen erheblichen Grundrechtseingriff ohne gesetzliche Rechtsgrundlage handeln.

Theoretisch Verhaltensprofile möglich

Auch eine „Selbstbeschränkung" von Wasserversorgern, digitale Zusatzfunktionen nicht nutzen zu wollen und nur die bisherige Ablesetaktung vorzunehmen, wäre ohne gesetzliche Verarbeitungsbefugnis rechtswidrig. Denn die Selbstbeschränkung eines Wasserverbandes zum zukünftigen Auslesen würde nichts daran ändern, dass durch dessen digitalen Wasserzähler bereits durch das Speichern neuer Datenkategorien eine Verarbeitung ohne Rechtsgrundlage erfolgen würde.

Detailregelung oder Satzungsermächtigung

Für den künftigen Einsatz digitaler Wasserzähler mit mehr als monatlicher Ablesemöglichkeit bzw. neuen Datenkategorien ist zeitnah eine Rechtsgrundlage erforderlich. Ich fordere den niedersächsischen Gesetzgeber dringend auf, eine bereichsspezifische Gesetzesregelung zu schaffen. Diese sollte detailliert vorgeben, welche Verbrauchswerte gespeichert und ausgelesen werden dürfen. Auch die Taktung der Auslesemöglichkeit sollte vom Gesetzgeber geregelt werden.

Als weitere Möglichkeit könnte sich der niedersächsische Gesetzgeber – in Anlehnung an die bayerische Lösung gemäß Art 24 Abs. 4 Gemeindeordnung Bayern – auch für eine bloße gesetzliche Satzungsermächtigung entscheiden. In diesem Fall würden nur die Grundsatzentscheidungen vom Gesetzgeber getroffen werden, die Details innerhalb dieses Rahmens würden die örtlichen Wasserversorger in ihren Satzungen regeln. Wichtig ist in diesem Fall, dass eine bloße Satzungsregelung der Wasserversorger ohne gesetzliche Satzungsermächtigung nicht genügt. Aufgrund der starken Eingriffsintensität bedarf es einer Satzungsermächtigung des Gesetzgebers, der hierbei die Grundentscheidungen trifft.

Keine weiteren Funktionen zulässig

Entscheidend ist letztlich, dass digitale Wasserzähler nur die Daten verarbeiten können (einschließlich Speicherung), die von einer gesetzlichen Rechtsgrundlage abgedeckt sind. Ein digitaler Wasserzähler, der mehr Daten verarbeitet, wäre unzulässig. Es käme für die Rechtswidrigkeit nicht darauf an, ob die Wasserversorger solche überschießenden Datenspeicherungen auch tatsächlich auslesen wollen.

Wasserversorger sind über Lücke informiert

Ich habe die niedersächsischen Spitzenverbände der Wasserversorger darüber unterrichtet, dass gegenwärtig für digitale Wasserzähler mit den genannten zusätzlichen Möglichkeiten keine gesetzliche Rechtsgrundlage in Niedersachsen existiert. Gegenüber dem Niedersächsischen Innenministerium habe ich die Erwartung geäußert, dass zeitnah eine hinreichende gesetzliche Grundlage geschaffen wird.

J.5. Schule

5.1 Niedersächsische Bildungscloud – ein digitaler Marathon

Das Niedersächsische Kultusministerium hat bereits Anfang 2017 erklärt, den Schulen mit der Niedersächsischen Bildungscloud (NBC) eine zentrale, digitale Lernplattform anzubieten und den Verein N-21: Schulen in Niedersachsen online e.V. mit der Entwicklung beauftragt. Ich habe bereits frühzeitig die datenschutzrechtliche Begleitung dieses Projekts angeboten.

Keine Transparenz der Datenflüsse

Anfang 2020 legte mir das Niedersächsische Kultusministerium erstmals ein Datenschutzkonzept zur NBC vor, das allerdings für eine datenschutzrechtliche Prüfung ungeeignet war. Insbesondere fehlte es an einer transparenten Beschreibung der Datenflüsse innerhalb der Bildungscloud sowie zwischen den am Betrieb beteiligten Akteuren. Auch wies die Dokumentation der vorgesehenen technisch-organisatorischen Maßnahmen sowie die der erforderliche Datenschutz-Folgenabschätzung (DSFA) erhebliche Defizite auf.

Das Datenschutzkonzept für die NBC sollte eine umfassende und systematische Dokumentation der datenschutzrelevanten Aspekte dieser komplexen Anwendung liefern. Damit kommt die verantwortliche Stelle ihren Rechenschaftspflichten gemäß der Datenschutz-Grundverordnung (DS-GVO) nach und schafft eine notwendige Grundlage für datenschutzrechtliche Prüfungen. Bedauerlicherweise war in dieser ersten Fassung kein DS-GVO-konformer, methodischer Ansatz sichtbar und es fehlte an wichtigen Dokumentationsinhalten. Ich teilte dem Kultusministerium die Mängel im Februar 2020 schriftlich mit.

Auch erste Überarbeitung enthält Defizite

Im Juni 2020 wurde mir eine überarbeitete Fassung des Datenschutzkonzepts vorgelegt. Doch auch diese wies weiterhin erhebliche Defizite auf, die eine Prüffähigkeit des Konzepts ausschlossen. Nach einer mündlichen Erörterung im Herbst 2020 nahm das Kultusministerium eine organisatorische Änderung im Rahmen der Konzepterstellung vor und sagte zu, das Datenschutzkonzept überarbeiten zu lassen.

Zahlreiche Defizite werden ausgeräumt

Ein wiederum überarbeitetes Dokument wurde mir im November 2020 vorgelegt. Gegenüber den bisher vorgelegten Unterlagen war darin die Darstellung der NBC nun deutlich transparenter und es wurden zahlreiche Defizite ausgeräumt. So wurde klar beschrieben, welche Maßnahmen als Folgen der DSFA zur Behandlung der Risiken tatsächlich umgesetzt worden waren. Zudem wurden nun nicht nur die Gewährleistungsziele der Informationssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit), sondern auch die vier verbleibenden Gewährleistungsziele Datenminimierung, Transparenz, Intervenierbarkeit und Nichtverkettung abgesichert. Ich prüfte dieses Dokument und teilte dem Kultusministerium im Dezember 2020 das Ergebnis meiner Prüfung mit.

Neues Dokument ist geeignete Grundlage

Grundsätzlich ist der Aufbau dieser Dokumentation nun eine geeignete Grundlage für eine DSFA der datenschutzrechtlich verantwortlichen Schulen. Jedoch sind einige meiner Anforderungen noch nicht umgesetzt. Dies betrifft insbesondere eine nachvollziehbare Darstellung der Datenflüsse und des Zusammenwirkens der an der NBC beteiligten Akteurinnen und Akteure sowie die Sicherstellung der Datenschutzkonformität von Produkten etwaiger Drittanbieter, deren Einbindung in die NBC grundsätzlich möglich ist.

Ausblick

Sobald die genannten Anforderungen umgesetzt sind, werde ich die für den Betrieb der NBC obligatorische DSFA eng begleiten. Zum datenschutzkonformen Betrieb der NBC unter rechtlichen und technischen Voraussetzungen werde ich eine Aussage treffen, nachdem das Datenschutzkonzept entsprechend meiner Anmerkungen überarbeitet worden ist.

5.2 Sicherheitslücken bei der HPI-Schul-Cloud

Durch eine anonyme Meldung sowie durch Medienberichte wurde ich im Mai 2020 darauf aufmerksam, dass die vom Hasso-Plattner-Institut betriebene Schulcloud (HPI-Schul-Cloud) erhebliche Sicherheitslücken aufweisen soll. Da die Niedersächsische Bildungscloud (NBC) auf der HPI-Cloud beruht, stand zu befürchten, dass auch personenbezogene Daten niedersächsischer Schülerinnen und Schüler betroffen sein könnten.

Über cloudbasierte Lernplattformen können für Schülerinnen und Schülern Lerninhalte bereitgestellt und Unterricht organisiert werden. Zudem besteht die Möglichkeit, dass Lernende und Lehrende über die Cloud miteinander kommunizieren. Eine Schule, die eine solche Cloud einsetzt, ist für die Verarbeitung der personenbezogenen Daten innerhalb der Cloud datenschutzrechtlich verantwortlich[1]. Bei der NBC handelt es sich um eine Lernplattform, die im Wesentlichen auf der HPI-Schul-Cloud basiert und deren Grundfunktionen von der HPI-Schul-Cloud abgedeckt werden.

Datenregen aus der Cloud

Tatsächlich waren innerhalb der HPI-Schul-Cloud Sicherheitslücken aufgetreten. Durch offen im Internet verfügbare Registrierungslinks bestand die Möglichkeit für unberechtigte Dritte, sich als Nutzer der HPI-Schul-Cloud zu registrieren und so Einblick in Listen mit Vor- und Zunamen der ebenfalls registrierten Schülerinnen und Schüler zu bekommen. Zudem war das sogenannte Ticketsystem der HPI-Cloud so konfiguriert, dass Meldungen zu technischen Problemen, die Rückschlüsse auf den jeweiligen Nutzer zulassen, von jedermann eingesehen werden konnten.

Meldungen aus Ticketsystem einsehbar

Über diese Sicherheitslücke war es unbefugten Dritten möglich, personenbezogene Daten von Schülerinnen und Schülern, die die HPI-Schul-Cloud bzw. die NBC nutzen, einzusehen.

Da diese Offenlegung der personenbezogenen Daten weder von einer gesetzlichen Rechtsgrundlage noch von der Einwilligung der betroffenen Schülerinnen und Schüler abgedeckt war, stellt sie eine Datenschutzverletzung dar. Schulen, welche die betroffenen Clouds einsetzen, sind verpflichtet, eine solche Verletzung der zuständigen Datenschutzaufsichtsbehörde zu melden[2].

Pflicht zur Meldung einer Datenpanne

1 Artikel 4 Nr. 7 Datenschutzgrundverordnung (DS-GVO)

2 Artikel 33 Absatz 1 DS-GVO

Auswirkungen auf die Niedersächsische Cloud

Auf Nachfrage teilte mir das Niedersächsische Kultusministerium im Mai 2020 mit, dass personenbezogene Daten niedersächsischer Schülerinnen und Schüler nicht betroffen gewesen seien. Aus dem Abschlussbericht einer anderen deutschen Datenschutzaufsichtsbehörde zum Vorfall innerhalb der HPI-Schul-Cloud ging jedoch hervor, dass auch fünf niedersächsische Schulen betroffen gewesen sein sollen, die die NBC und damit auch Bestandteile der HPI-Schul-Cloud einsetzen. Daraufhin bat ich sowohl das Kultusministerium als auch die betroffenen Schulen um Stellungnahme und forderte sie dazu auf, der Verpflichtung zur Meldung einer Datenschutzverletzung nachzukommen.

Auch niedersächsische Schulen betroffen

Aus den Rückmeldungen der Schulen war zu entnehmen, dass die Nutzung der NBC ab Kenntnis der Sicherheitslücke zunächst eingestellt worden war, bis die Lücke behoben war. Das Kultusministerium teilte zudem mit, dass in Folge der Sicherheitslücke der Betrieb der NBC für einige Wochen ausgesetzt worden sei, um alle Sicherheitsfragen klären und datenschutzkonforme Zustände herstellen zu können.

Lücken wurden geschlossen

Der Umstand, dass für das Niedersächsische Kultusministerium zunächst unklar war, ob niedersächsische Schulen von der Sicherheitslücke überhaupt betroffen waren, zeigt die Komplexität des Zusammenspiels zwischen HPI-Schul-Cloud und NBC. Das Kultusministerium teilte mir im Zuge seiner Stellungnahme mit, dass die Sicherheitslücken zwischenzeitlich geschlossen wurden, sodass die im NBC wieder für die Schulen nutzbar ist, die im Rahmen des Pilotprojekts beteiligt sind.

5.3 Fragebögen zur Schuleingangsuntersuchung

Im Rahmen der Schuleingangsuntersuchung dürfen die zuständigen Gesundheitsämter nur die personenbezogenen Daten von den Eltern erheben, die auch für die Durchführung der Untersuchung erforderlich sind. Darüber hinaus gehende Daten dürfen nur auf freiwilliger Basis erhoben werden.

Ein Landkreis hat im Zuge der Schuleingangsuntersuchung nicht erforderliche personenbezogene Daten der Eltern eines Schülers verpflichtend abgefragt. So wurden neben Fragen zu Vorerkrankungen und Entwicklung des Kindes auch Fragen zur Schulbildung, Berufsausbildung und Berufstätigkeit der Eltern gestellt. Ein betroffener Elternteil hat hiergegen eine datenschutzrechtliche Beschwerde erhoben – mit Erfolg.

Fit für die Schule?

Vor der Einschulung wird im Rahmen des Schulaufnahmeverfahrens der Entwicklungs- und Gesundheitszustand des Kindes ärztlich überprüft. Diese gesetzlich vorgeschriebene Schuleingangsuntersuchung dient der Feststellung der Schulfähigkeit angehender Schülerinnen und Schüler[1]. Zuständig für die Durchführung der Untersuchung sind die Landkreise sowie die kreisfreien Städte[2]. Die Untersuchung wird dort von den jeweiligen Gesundheitsämtern durchgeführt.

Auskunftspflicht der Erziehungsberechtigten

Für die Beurteilung der Schulfähigkeit werden auch Angaben benötigt, die zum Beispiel die Entwicklung und frühere Erkrankungen des Kindes betreffen. Hierzu bedarf es bestimmter Auskünfte der Eltern an das Gesundheitsamt, die verpflichtend zu erteilen sind[3]. Diese werden mit Hilfe eines Fragebogens im Vorfeld der Schuleingangsuntersuchung erhoben.

Nur Daten für Einschätzung der Schulfähigkeit sind verpflichtend

Bei den zu erteilenden Auskünften handelt es sich um personenbezogene Daten des Kindes bzw. von dessen Eltern. Die Verarbeitung dieser Daten – hier durch das Gesundheitsamt – kann grundsätzlich auf die Regelung des § 56 Absatz 1 Satz 2 Nds. Schulgesetz gestützt werden. Es dürfen jedoch nur solche Auskünfte verpflichtend abgefragt werden, die auch zur Feststellung der Schulfähigkeit erforderlich sind. Personenbezogene Daten, die für die Einschätzung der Schulfähigkeit lediglich hilfreich, jedoch hierfür nicht zwingend notwendig sind, dürfen nicht erhoben werden.

1 § 56 Absatz 1 Satz 1 Nr. 1 Nds. Schulgesetz.

2 § 5 Absatz 2 Satz 1 Nds. Gesetz über den öffentlichen Gesundheitsdienst.

3 § 56 Absatz 1 Satz 2 Nds. Schulgesetz

Die Erhebung von Daten bezüglich Schulbildung, Berufsausbildung und Berufstätigkeit der Eltern (sogenannte sozialmedizinische Daten) kann mangels Erforderlichkeit nicht auf eine gesetzliche Rechtsgrundlage gestützt werden und darf nur mit Einwilligung der Eltern auf freiwilliger Basis erfolgen. Hierbei ist insbesondere darauf zu achten, dass auf dem Fragebogen der Bereich der freiwillig zu machenden Angaben optisch deutlich vom Bereich der Pflichtangaben abgegrenzt wird.

Landkreis sagt Änderungen zu

Muster sollen verbessert werden

Im Rahmen des erwähnten datenschutzrechtlichen Prüfverfahrens sagte der betroffene Landkreis zu, den Vorbereitungsbogen abzuändern. Die Fragen zu Schulbildung, Berufsausbildung sowie Berufstätigkeit der Eltern würden künftig deutlich als freiwillige Angabe gekennzeichnet werden.

Zudem habe ich das Niedersächsische Landesgesundheitsamt auf das Problem der überbordenden Datenerhebung durch bestehende Musterfragebögen hingewiesen. Ich stehe mit dem Amt wegen einer landesweiten datenschutzkonformen Gestaltung der Muster im Kontakt.

J.6. Wirtschaft

6.1 Nachkontrollen zur Querschnittsprüfung: Nach der Prüfung ist vor der Prüfung

Ende Juni 2018 hatte ich eine branchenübergreifende Prüfung von 50 niedersächsischen Unternehmen zur Umsetzung der Datenschutz-Grundverordnung (DS-GVO) eingeleitet und hierüber auch in den vergangenen beiden Tätigkeitsberichten ausführlich informiert. Nach zwei Prüfungsschritten gab es immer noch Unternehmen, in denen ich erhebliche Defizite feststellen musste. In fünf von ihnen habe ich im vergangenen Jahr, wie vorab angekündigt, weitergehende Kontrollen durchgeführt.

Abschlussbericht der Prüfung (November 2019): https://t1p.de/Querschnittspruefung

Ende 2019 informierte ich die Unternehmen, dass ich im Rahmen der weitergehenden Prüfung auch eine Vor-Ort-Kontrolle durchführen werde, die voraussichtlich zwei Tage in Anspruch nehmen würde. Ich benannte die Prüfungstage und bat um Anwesenheit der Geschäftsführung, der bzw. des betrieblichen Datenschutzbeauftragten sowie eines Beschäftigten aus dem Bereich IT. Zudem setzte ich die Unternehmen darüber in Kenntnis, dass ich an den Prüfungstagen auch eine Begehung der Betriebsstätte(n) einschließlich Serverraum, beabsichtigte. Auch bat ich um die Zurverfügungstellung geeigneter Räumlichkeiten. Zur schriftlichen Vorbereitung bat ich die Unternehmen mir verschiedene Fragen, insbesondere zu den Bereichen Videoüberwachung und Beschäftigtendatenschutz zu beantworten. Die Auskünfte sollten im Vorfeld zur Vor-Ort-Kontrolle gegeben werden, damit diese mit einbezogen werden konnten.

Prüfung vor Ort statt nur per Post

Zahlreiche Unterlagen und Präsentation gefordert

Für den Prüfungstermin selbst bat ich die Unternehmen verschiedene Unterlagen bereit zu halten, mit denen diese die Einhaltung der datenschutzrechtlichen Grundsätze für die Verarbeitung personenbezogener Daten im Rahmen ihrer Rechenschaftspflicht nachweisen können. Hierzu zählen u.a. ein Verzeichnis der Verarbeitungstätigkeiten, Verträge zur Auftragsverarbeitung sowie ein Löschkonzept.

Für die Prüfung des technisch-organisatorischen Datenschutzes erbat ich eine Präsentation, in der in strukturierter Art und Weise die Verfahren bzw. das Verzeichnis der Verarbeitungstätigkeiten inhaltlich zu erläutern waren. Dabei sollte anhand von drei Verfahren exemplarisch aufgezeigt werden, welche Risiken vom Unternehmen identifiziert worden waren, inklusive Eintrittswahrscheinlichkeit, Schadenhöhe und der geeigneten technischen sowie organisatorischen Schutzmaßnahmen. Bei den ausgewählten Verfahren sollte es sich um solche handeln, bei denen nach unternehmensseitiger Einschätzung die größten Risiken für die Rechte und Freiheiten natürlicher Personen bestehen oder bei denen eine Datenschutz-Folgeabschätzung durchgeführt worden war. Zur Prüfung bereitzuhalten waren außerdem Unterlagen zur Systemlandschaft, dem Berechtigungskonzept, der Verschlüsselung, Anonymisierung oder Pseudonymisierung sowie das Datensicherungskonzept.

Große Unterschiede bei den Kontrollen vor Ort

Die Unternehmen waren Ende August 2019 darüber informiert worden, dass ich im Herbst 2019 die Einleitung eines aufsichtsbehördlichen Prüfverfahrens samt Vor-Ort-Kontrolle beabsichtigte. Zwischen der konkreten Ankündigung und dem Vor-Ort-Termin lag im Minimum ein Monat, meist sogar deutlich mehr Zeit. Einige Unternehmen nutzen diese Zeit, andere bereiteten sich praktisch nicht auf die Prüfung vor.

So war beim ersten Besuch eines Unternehmens kein Raum für die Besprechung vorbereitet worden. Der betriebliche Datenschutzbeauftragte wurde erst nach mehrmaliger Bitte zum Termin hinzugezogen. Die nach dem Einleitungsschreiben bereitzuhaltenden Dokumentationen waren nicht vorhanden, andere Unterlagen zeigten keine transparente Darstellung der verarbeiteten Kundendaten.
Auch bei einem anderen Unternehmen fiel die Dokumentation unzureichend aus. Ebenso entsprachen die erbetenen Präsentationen des technisch-organisatorischen Datenschutzes nicht immer meinen Erwartungen.

Es gab aber auch Unternehmen, die sich sehr gut und mit professioneller Unterstützung ihres Datenschutzbeauftragten auf die Vor-Ort-Kontrolle vorbereitet hatten. So konnten sie zugleich ihrer Rechenschaftspflicht aus der Datenschutz-Grundverordnung nachkommen.

Unternehmen hatten nicht mit Vor-Ort-Kontrolle gerechnet

Bei nahezu allen Besuchen zeigte sich, dass die verantwortlichen Stellen nicht mit einer Kontrolle vor Ort gerechnet hatten, insbesondere, wenn sie weit weg von Hannover oder im ländlichen Raum angesiedelt waren. Allein das wird also dafür sorgen (auch bei anderen Unternehmen vor Ort bzw. aus der jeweiligen Branche), dass die Datenschutzaufsichtsbehörde nachhaltig und dauerhaft in Erinnerung bleibt. Den Unternehmen wurde deutlich, dass die Aufsichtsbehörde auch im Flächenland Niedersachsen jederzeit erscheinen kann.
Zugleich war mir ein vertiefter Einblick in sehr unterschiedliche Geschäftsmodelle mit ihren differenzierten Datenverarbeitungsprozessen möglich.

Auswertung und Ausblick

Die Ergebnisse der Vor-Ort-Kontrollen wurden anschließend von den juristischen und technischen Referaten innerhalb meiner Behörde ausgewertet. Das sehr widersprüchliche Bild der Besuche in den Unternehmen spiegelte sich auch hier wieder.

Die Unternehmen initiierten bereits während dieser Auswertungsphase erste Prozesse zur datenschutzkonformen Änderung der während der Vor-Ort-Kontrollen aufgezeigten Defizite. Diese wurden den Unternehmen vor Ort und durch die direkten Gespräche deutlicher als dies im Rahmen eines schriftlichen Verfahrens möglich gewesen wäre.

Breites Spektrum der Ergebnisse

Nach Zusammenführung der Auswertungen konnten einige Prüfungen abgeschlossen werden, da nur geringe Änderungen und Anpassungen notwendig waren. Hier konnten weitere aufsichtsbehördliche Maßnahmen im Zusammenwirken mit den Unternehmen vermieden werden, indem ich Hinweise zur Abstellung bestimmter Defizite gab und den Unternehmen die Möglichkeit zur Änderung einräumte.

Andere Unternehmen ersuchte ich um die konkrete Umsetzung und deren Dokumentation unter der Ankündigung andernfalls weitere aufsichtsbehördliche Maßnahmen zu ergreifen. Gemeint waren damit insbesondere Anweisungen, aber auch eine Beschränkung bzw. ein Verbot der Verarbeitung.

Schließlich gab es auch Prüfungen, bei denen verschiedene gravierendere Verstöße gegen das Datenschutzrecht festgestellt wurden.
Hier ergingen Anhörungsschreiben, in denen ich die beabsichtigten Maßnahmen im Rahmen einer verwaltungsrechtlichen Anhörung dezidiert darstellte. Diese umfassten Anweisungen und Anordnungen, welche auch Verarbeitungsverbote einschlossen.

Bei wenigen verantwortlichen Stellen wird die Prüfung noch 2021 fortgesetzt werden müssen. Positiv festzuhalten ist, dass zumindest nach der Vor-Ort-Kontrolle auch in bislang defizitär aufgestellten Unternehmen erkannt wurde, dass den datenschutzrechtlichen Versäumnissen nicht mit Bordmitteln abzuhelfen ist, sondern professionelle Unterstützung notwendig ist.

Unternehmen müssen Kosten des Verfahrens tragen

Die Kosten des Verfahrens sind von den Unternehmen zu tragen, da es sich bei den Prüfungen zur Umsetzung der DS-GVO um eine Amtshandlung handelt, zu der die Unternehmen aufgrund der Ergebnisse der Querschnittsprüfung Anlass gegeben hatten. Die Einhaltung der datenschutzrechtlichen Vorschriften gehört zu deren gesetzlich normierten Pflichten.

Prüfungen vor Ort werde ich auch zukünftig durchführen. Abhängig vom konkreten Fall können Erkenntnisse so schneller gewonnen werden. Zugleich wird den Unternehmen auf diese Weise die Möglichkeit geboten in einen persönlichen Dialog zu treten.

6.2 Bank klassifiziert Kunden

Am 29. Januar 2020 veröffentlichte die Hannoversche Allgemeine Zeitung einen Artikel darüber, dass die Schufa die Daten von 220.000 Kunden einer Hannoveraner Bank untersucht habe. Das Geldinstitut soll mit Hilfe der Auskunftei die Daten analysiert haben, um den besten Kommunikationsweg mit der Kundschaft zu ermitteln.

Die besagte Bank wollte den bestmöglichen Kommunikationsweg zu ihren Kundinnen und Kunden ermitteln, ohne ihn bei diesen direkt zu erfragen. Hierfür soll die Bank Datensätze aller Kundinnen und Kunden bei der Schufa Holding AG abgefragt haben. Nach einem Datenabgleich mit den bei der Schufa gespeicherten Daten sollte als Ergebnis feststehen, wie die Bank am besten mit ihrer Kundschaft in Kontakt treten kann.

Kundschaft wird von der Schufa informiert

Öffentlich wurde die Angelegenheit, weil Kundinnen und Kunden, die einen zahlungspflichtigen Account bei der Schufa besitzen, über eine Datenanfrage des Kreditinstituts bei der Schufa informiert wurden und sich an die örtliche Presse wandten. Die Kundinnen und Kunden der Schufa mit Premium Account erhielten eine Information per E-Mail mit dem Inhalt „Bank XY hat eine neue Anfrage gestellt".

Zahlreiche Beschwerden von Betroffenen

Bereits vor Veröffentlichung des Zeitungsartikels hatte mich die Beschwerde eines betroffenen Kunden erreicht, der ebenfalls von der Schufa über die Datenanfrage der Bank informiert worden war.

In Folge der Zeitungsveröffentlichung erhielt ich noch eine Vielzahl weiterer Beschwerden betroffener Personen, die Kundinnen und Kunden der Bank sind oder waren oder nur als Kontobevollmächtigte eine Beziehung zum Geldinstitut haben. Bereits unmittelbar nach Eingang der ersten Beschwerde leitete ich ein aufsichtsbehördliches Prüfverfahren ein und begann mit meinen Ermittlungen.

Mögliche Rechtsgrundlage nach der DS-GVO

Bank beruft sich auf berechtigtes Interesse

Das Geldinstitut beruft sich bei der Datenübermittlung an die Auskunftei auf Art. 6 Abs. 1 lit. f) der Datenschutz-Grundverordnung (DS-GVO). Danach können personenbezogene Daten verarbeitet und weitergegeben werden, wenn ein „berechtigtes Interesse" vorliegt. Die Einwilligung eines Kunden oder einer Kundin in die Verarbeitung wäre in diesem Falle nicht erforderlich.

Ob dieses „berechtigte Interesse" für diese Datenzusammenführung mit anschließendem Profiling auch gegeben ist, wenn ein Geldinstitut wissen möchte, ob es seine Kundschaft per Brief oder per E-Mail kontaktieren möchte, ist Gegenstand des von mir eingeleiteten Prüfverfahrens.

Initiative ging von der Schufa aus

Die Datenanalyse seines Kundenbestands wurde dem Bankhaus von der Schufa als Verbesserungsmaßnahme zur Kundenkommunikation angeboten. Die Schufa versicherte, dass diese Aktion keine Auswirkungen auf die Bonitäts-Scores der Bankkunden und -kundinnen habe. Das Geldinstitut nahm nach eigener Aussage das Angebot der Auskunftei an, da eine direkte Umfrage weniger erfolgversprechend, zeitaufwändiger und erheblich kostenintensiver gewesen wäre.

Gruppen für die verbesserte Ansprache

Die Zusammenarbeit zwischen Bank und Auskunftei hatte das Ziel die Bankkundschaft in drei Gruppen für die Kontaktaufnahme einzuteilen, z.B. um Bankprodukte zielgenauer anbieten zu können.

Digital-affin, Filial-affin oder Hybrid?

Die Schufa verfügt über umfangreiche Daten der Bürgerinnen und Bürger, die deren Leben abbilden, so zum Beispiel Bankverbindungen, Kreditkarten, (Online-) Kredite, Handyverträge, Ratenkäufe und Leasingverträge. Die Analyse der übermittelten Daten sollte im Endeffekt eine Kategorisierung der Kundschaft in „digital-affin", „Filial-affin" und „Hybrid-Kunde/Kundin" ergeben. Daraus ließe sich im Zusammenspiel mit den eigenen Kundendaten für die Bank ableiten, dass es nicht sinnvoll ist, einer eigentlich digital-affinen Kundin werbliche Angebote per Post zuzusenden.

Zu als Filial-affin eingestuften Kunden und Kundinnen würde dann durch einen Bankberater Kontakt aufgenommen und diese würden zum Gespräch in die Filiale eingeladen. Digital-affine Kundinnen und Kunden erhielte produktbezogene E-Mails oder Mitteilungen in ihr bankinternes Online-Postfach eingespielt, wohingegen die Hybrid-Kundschaft wiederum sowohl digital als auch über die Bankfiliale angesprochen werden könnte.

Undurchsichtige Kundeninformation

Das Geldinstitut gab gegenüber Medien sowie im Kontrollverfahren an, dass es seine Kundschaft über diese Einteilung in Gruppen informiert hätte. Hierfür hatte die Bank einen ca. 30-seitigen Brief versendet, in dem lediglich in einem Absatz die Zusammenarbeit mit der Schufa zur Verbesserung des Kundenkontakts Erwähnung fand. In diesem Rahmen wurden die Kundinnen und Kunden auch daraufhin gewiesen, dass sie der Datenverarbeitung und der Analyse widersprechen könnten.

Dass die Kundinnen und Kunden auch von der Schufa über die Aktion informiert werden, war der Bank bis zum Eingang der ersten telefonischen Nachfragen im hauseigenen Callcenter unbekannt.

Handlung im „völligen Kundeninteresse"

Bank sieht auch positive Effekte für die Umwelt

Sowohl Schufa als auch die Bank behaupten in Pressestellungnahmen mit dieser Aktion überwiegend im Interesse der Kundinnen und Kunden und der Umwelt gehandelt zu haben. Die Kundschaft hätte ein Interesse daran, mit werblichen Angeboten so angesprochen zu werden, wie es ihren Vorzügen entspricht. Die beteiligten Unternehmen führen ferner ins Feld, dass die somit nicht mehr postalisch versandten Werbebriefe viel Papier einsparen würden. Diese Aktion hätte also auch im Sinne der Nachhaltigkeit einen positiven Effekt.

Stand des Prüfverfahrens

Im Verlauf des aufsichtsbehördlichen Prüfverfahrens habe ich zu prüfen, ob die Datenübermittlung der aufbereiteten Kundendaten von der Bank an die Schufa Holding AG nach der DS-GVO rechtmäßig erfolgte. Dabei sind die vorgetragenen Argumente sorgfältig einzuschätzen und abzuwägen. Aufgrund des komplexen Sachverhalts, mehrerer an der Aktion beteiligter Unternehmen und einer Vielzahl betroffener unterschiedlicher Kundengruppen dauerten meine Ermittlungen bei Redaktionsschluss noch an.

6.3 Datenschutz in der GmbH & Co. KG

Gesellschafter einer Kommanditgesellschaft haben gegenüber dem Komplementär einen Herausgabeanspruch der ladungsfähigen Anschriften ihrer Mitgesellschafter. Damit ist gewährleistet, dass Kommanditisten sich über die Zusammensetzung des Gesellschafterkreises informieren können, um zum Beispiel mögliche Stimmverbote überprüfen oder Gesellschafterrechte ausüben zu können.

Ein Schiffsbeteiligungsfonds wurde nach der Finanzkrise 2008/2009 als antizyklischer „Blindpool"-Schifffonds aufgelegt. Die Anlegerinnen und Anleger investieren bei einem Blindpool - als Eigenschaft eines geschlossenen Fonds - in diesem Sinne „blind", so dass ihnen die konkreten Investitionsziele anfangs nicht bekannt sind. Ziel war es in diesem Fall, die aus der Finanzkrise hervorgegangene Schifffahrtskrise als Gelegenheit zu nutzen, um nach Erholung des Welthandels für die Anleger hohe Renditen mit der Beteiligung an Schiffen zu erzielen.

Der Fonds wurde in der Rechtsform einer Kommanditgesellschaft mit einer Unternehmergesellschaft (haftungsbeschränkt) als Komplementär (Vollhafter) aufgesetzt, hier mit einer Schiffsbeteiligungs-Unternehmergesellschaft (haftungsbeschränkt) und Co. KG, an der sich Anleger als Kommanditisten durch Anteilskauf an der KG beteiligen konnten. Der Vertrieb erfolgte über einen bundesweit tätigen Finanzdienstleister. Die Prognosen konnten allerdings nicht eingehalten werden, die Anlegerinnen und Anleger erlitten in den Folgejahren schwere Verluste.

Gesellschafter versucht mit anderen Anlegern in Kontakt zu treten

Kommanditisten wollen Fonds auflösen

Um den drastischen Verlusten Einhalt zu gebieten wollten einige - bereits untereinander bekannte - Kommanditisten die Komplementärin, also die Geschäftsführungsgesellschaft zur Liquidation des Fonds zwingen. Die Erlöse durch die Schiffsverkäufe sollten an die Anlegerinnen und Anleger zurückgezahlt werden, damit wenigstens ein Bruchteil der ursprünglichen Anlagesumme hätte gerettet werden können. Hierzu wählte die Anlegergruppe einen Kommanditisten aus ihren Reihen, der gegen die aktuelle Geschäftsführung der Komplementärgesellschaft vorgehen sollte. Allerdings benötigte er hierfür das Mandat weiterer Mitgesellschafter, um bei einer einzuberufenden Gesellschafterversammlung genug Stimmrechte auf sich zu vereinen, damit eine Fondsauflösung betrieben werden kann.

Mitgesellschafter werden per E-Mail kontaktiert

Bereits in der Vergangenheit hatte die Anlegergruppe über eine Treuhänderin der Beteiligungsgesellschaft eine Liste mit Kontaktdaten, wie Anschriften, E-Mail-Adressen und Telefonnummern der übrigen Mitgesellschafter erhalten. Diese Adressliste wurde nun von dem ausgewählten Vertreter genutzt, sämt-

liche Mitgesellschafter per E-Mail-Rundschreiben zu kontaktieren, um von ihnen unter Hinweis auf die aussichtslose Lage des Schifffonds eine weitreichende Bevollmächtigung für die Ausübung von Stimmrechten zu erbitten.

Fondsverwalter holt zum Gegenschlag aus

Die Geschäftsführung der Komplementärgesellschaft erfuhr von diesem Vorgehen, da sich vom Vertreter angeschriebene Anleger besorgt an sie wendeten. Die Komplementärin sah in der Kontaktaufnahme der Kommanditisten untereinander einen offenkundigen Datenmissbrauch und brachte ihrerseits weite Teile der Gesellschafterrunde dazu bei mir einen Datenschutzverstoß des Vertreters anzuzeigen.
Hierfür wurde den Anlegerinnen und Anlegern, die die missbräuchliche Nutzung ihrer personenbezogenen Daten anzeigen wollten, ein vorformuliertes Schreiben zur Verfügung gestellt. Es mussten nur noch Adresse und Unterschrift ergänzt werden.

Das Schreiben sollte an den Vertreter der Kommanditistengruppe und an die Landesbeauftragte für den Datenschutz Niedersachsen gerichtet werden. Auf diese Weise erreichten mich 36 Beschwerden gegen den Absender der E-Mail. In dem Formschreiben wurde gegenüber dem Vertreter angezeigt, dass personenbezogene Daten wie Anschriften, E-Mail-Adressen und Telefonnummern ohne Einwilligung verarbeitet worden waren, deren Herkunft beauskunftet und die Kontaktdaten gelöscht werden sollten.

Zahlreiche Beschwerden gegen den Absender der E-Mail

Kontaktaufnahme rechtlich zulässig, aber auf andere Weise

In dem eingeleiteten aufsichtsbehördlichen Prüfverfahren stellte ich fest, dass lediglich wegen der Verwendung der E-Mail-Adressen ein datenschutzrechtlicher Verstoß des Verantwortlichen, hier des Vertreters vorlag, da ihm eine Einwilligung der Betroffenen zur Verarbeitung der E-Mail-Adressen nicht vorlag. Der Initiator der Rund-Mail wurde daher von mir verwarnt. Eine Löschung der zu Unrecht verarbeiteten Daten wurde im Verfahren von ihm zugesichert und die Betroffenen wurden darüber von ihm informiert.

Nichtsdestotrotz muss es datenschutzkonform möglich sein, dass Mitwirkungsrechte von Gesellschaftern effektiv ausgenutzt werden können. Jeder Kommanditist hat gegen die Gesellschaft, Adressat ist mithin die Komplementärin, einen Anspruch auf Herausgabe der ladungsfähigen (postalischen) Anschriften aller Mitkommanditisten. Damit ist gewährleistet, dass Kommanditisten sich über die Zusammensetzung des Gesellschafterkreises informieren können, um zum Beispiel mögliche Stimmverbote überprüfen oder Gesellschafterrechte ausüben zu können. Ein Anspruch auf das Abfragen und die Weiterverwendung von E-Mail-Adressen der Mitgesellschafter ohne deren Einwilligung besteht allerdings nicht.

Verwendung der Postadresse ist datenschutzkonform

Die Verarbeitung der ladungsfähigen Anschriften der Mitkommanditisten ist zur Wahrung der berechtigten Interessen des einzelnen Kommanditisten gem. Art. 6 Abs. 1 Satz lit. f) Datenschutz-Grundverordnung (DS-GVO) datenschutzkonform. Denn Kommanditisten haben ein erhebliches Interesse an einer Kooperation mit den übrigen Mitgesellschaftern. Dieses Interesse überwiegt das vermeintliche Schutzinteresse der anderen Gesellschafter an einer Nichtoffenbarung ihrer ladungsfähigen Anschrift. Einer Zustimmung der übrigen Kommanditisten zur Verarbeitung ihrer ladungsfähigen Anschrift bedarf es folglich nicht.

Eine Verweigerung der Komplementärin, diese Informationen zu übermitteln, kann daher nicht mit der DS-GVO begründet werden. Darüber hinaus besteht die Möglichkeit der Einsichtnahme in das öffentlich zugängliche Handelsregister, um Vorname, Nachname, Einlagehöhe, Geburtsdatum und Geburtsort aller Kommanditisten einer KG in Erfahrung zu bringen.

6.4 „Energie-Pool“ für Positivdaten wechselwilliger Verbraucherinnen und Verbraucher

Gemeinsam sollen die Schufa Holding AG und die CRIF Bürgel GmbH laut Medienberichten eine Datenbank für Energieversorger entwickelt haben, über die sich das Wechselverhalten von Kundinnen und Kunden nachvollziehen lassen könnte. Verbraucherinnen und Verbraucher, Wechselportale und Verbraucherverbände befürchteten, der Zweck dieser Speicherung sei es, solche Kundinnen und Kunden zu identifizieren, die häufig ihre Verträge wechseln, um Prämien zu erhalten und diesen künftig lukrative Neukundenangebote zu verwehren.

Im Sommer 2020 recherchierten NDR und Süddeutsche Zeitung, dass im Energiesektor ein „Branchenpool“ geplant sei, der auch sogenannte Positivdaten von Kundinnen und Kunden enthält. Hierdurch besteht für Verbraucherinnen und Verbraucher die potenzielle Gefahr, dass Energieversorger wechselfreudige Kundinnen und Kunden identifizieren und ablehnen können, auch wenn diese sich stets vertragsgemäß verhalten haben. Diese Pläne wurden von verschiedenen Datenschutzaufsichtsbehörden sowie den Verbraucherzentralen kritisiert. Sie waren auch Gegenstand der Beratungen im Rahmen der Herbstsitzung des Arbeitskreises (AK) „Auskunfteien“ der Datenschutzaufsichtsbehörden.

Wechselkunden könnten im Nachteil sein

Verarbeitung von Positivdaten nur in engen Grenzen

Bereits der Beschluss „Verarbeitung von Positivdaten zu Privatpersonen durch Auskunfteien“ der Konferenz der Datenschutzaufsichtsbehörden von Bund und Ländern (DSK) aus dem Jahr 2018 beschäftigte sich mit diesem Thema. Positivdaten sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten beinhalten. Für die Verarbeitung solcher Daten legt der DSK-Beschluss hohe Hürden fest:

DSK-Beschluss: https://t1p.de/Positivdaten

Die Verarbeitung von Positivdaten darf grundsätzlich nur auf Grundlage einer Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a, Art. 7 Datenschutz-Grundverordnung (DS-GVO) erfolgen, wobei auf die Anforderungen an die Freiwilligkeit nach Art. 7 Abs. 4 DS-GVO hingewiesen wird. Allenfalls in engen Ausnahmefällen ist eine Rechtfertigung auf Grundlage der Interessenabwägung gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO möglich, und zwar ausschließlich für Kreditinstitute bei Verträgen mit einem kreditorischen Risiko.

Für das hier identifizierte Problem der Erfassung von Positivdaten innerhalb eines „Energie-Branchenpools“ kann sich die Verarbeitung nicht auf die Interessenabwägung stützen. Im Gegensatz zur Verarbeitung von Positivdaten im Bereich der Kreditvergabe existiert auf Seiten der Energieversorger kein ausreichend hohes kreditorisches Risiko, das ein berechtigtes Interesse begründen könnte.

Ausfallrisiko für Anbieter ist gering

Energieversorger können insbesondere durch entsprechende Vertragsgestaltung das kreditorische Risiko beeinflussen und von ihren Kundinnen und Kunden z. B. regelmäßige Abschlagszahlungen verlangen. Selbst wenn diese aufgrund einer zu niedrigen Schätzung im Einzelfall zu gering ausfallen, bleibt das Ausfallrisiko gering. Folglich ist auch bei dieser Konstellation kein ausreichend hohes Kreditrisiko gegeben. Gegenüber den wirtschaftlichen Interessen der Energieversorger sind darüber hinaus die Interessen der Verbraucherinnen und Verbraucher höher zu bewerten, zumal es nicht der Erwartungshaltung der Kundinnen und Kunden entspricht, dass ein vertragstreues Verhalten bei einer Auskunftei verarbeitet wird.
Die Verarbeitung von Positivdaten in einem Energie-Branchenpool auf Grundlage des Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist daher abzulehnen.

Entscheidung der Datenschutzkonferenz

Beschluss der DSK:
https://t1p.de/dsk-energie

Auch die DSK erklärte im März 2021 die Verarbeitung von Positivdaten von Kundinnen und Kunden von Energieversorgern für datenschutzrechtlich unzulässig. Sie stellte in ihrem Beschluss klar, dass der Wunsch „vermeintliche Schnäppchenjäger" in einem zentralen Datenpool zu erfassen, kein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 S. 1 lit. f. DS-GVO darstellt. Zudem würde ein solcher Datenpool der Liberalisierung auf dem Energiemarkt und dem damit ermöglichten Wettbewerb zuwiderlaufen.

6.5 Beschäftigtendatenschutz bei Amazon in Winsen

In der Logistikbranche werden zur Steigerung der Effizienz dauerhaft die Verfahrensabläufe überprüft. Besonders augenfällig ist dies im Bereich der Kurier-, Express- und Paketdienste. Dort wird mittlerweile die sogenannte „Same-Day Lieferung" am Tag der Bestellung einer Ware angeboten. Um diese kurzen Lieferzeiten zu erreichen, ist die Einbindung informations-technologischer Unterstützung unentbehrlich. Jedoch sind dabei stets die allgemein gültigen rechtlichen Vorgaben zum Schutz von Beschäftigtendaten zu beachten. Dass diese nicht immer eingehalten werden, zeigte sich im Berichtszeitraum bei der Amazon Logistik Winsen GmbH.

Voraussetzungen für die Verarbeitung von Beschäftigtendaten

Im Rahmen eines bestehenden Arbeitsvertrages dürfen Arbeitgeberinnen und Arbeitgeber Beschäftigtendaten nach § 26 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes (BDSG) grundsätzlich unter zwei Voraussetzungen verarbeiten:

1. Die Verarbeitung der Beschäftigtendaten muss grundsätzlich für den Zweck „Durchführung des Beschäftigungsverhältnisses" erfolgen, mit anderen Worten für die „Erfüllung des jeweiligen Arbeitsvertrages".
2. Darüber hinaus muss die Verarbeitung der konkreten Beschäftigtendaten für diesen Zweck stets erforderlich sein.

Unter den Begriff „verarbeiten" fallen laut der Definition in Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO) unter anderem die Erhebung und Nutzung von Beschäftigtendaten.

Darauf aufbauend sind z. B. die folgenden Datenverarbeitungen zulässig:

- Arbeitgeberinnen und Arbeitgeber haben aus dem Arbeitsvertrag die Pflicht, den Lohn der Beschäftigten zu bezahlen. Damit ist es erforderlich, dass sie deren Kontodaten verarbeiten.
- Darüber hinaus haben Arbeitgeberinnen und Arbeitgeber im Zusammenhang mit dem Arbeitsvertrag auch gesetzliche Pflichten, die es erforderlich machen, dass sie Beschäftigtendaten verarbeiten, wie etwa die Übermittlung von Lohnsteuerbescheinigungen der Beschäftigten an die Finanzverwaltung.
- Zudem erlaubt die unternehmerische Freiheit den Arbeitgeberinnen und Arbeitgebern im Rahmen ihres Weisungsrechts, gegenüber den Beschäftigten die Art und Weise der Erbringung der jeweiligen Arbeitsleistung, also Arbeitsabläufe, zu bestimmen. Folglich dürfen sie grundsätzlich die für die Gestaltung von Arbeitsabläufen erforderlichen Beschäftigtendaten erheben und nutzen.

  Arbeitgeber entscheidet über Art der Mail-Kommunikation

  Beispiele:
  - In einem mittelständischen Handwerksbetrieb entscheidet die Geschäftsführung, dass die Kommunikation mit Kundinnen und Kunden per E-Mail nur über eine allgemeine Mail-Adresse des Betriebs abgewickelt werden soll (handwerksbetriebs@mail.de). Nur die Geschäftsführung und/oder das Sekretariat des Handwerksbetriebes kommunizieren mit dieser Mail-Adresse unter Nennung von Vor- und Zunamen mit den Kundinnen und Kunden.

- In einem anderen mittelständischen Handwerksbetrieb entscheidet sich die Geschäftsführung, dass zusätzlich zu einer allgemeinen Mail-Adresse für den Betrieb alle Beschäftigten eine unternehmenseigene Mail-Adresse unter Nutzung des Vor- und Zunamens erhalten (vorname.name@handwerksbetrieb.de) sowie alle Beschäftigten mit den Kundinnen und Kunden unter Nennung der jeweiligen Vor- und Zunamen kommunizieren sollen. Auch diese Datenverarbeitung ist zulässig.

Allerdings wird das Recht der Arbeitgeberinnen und Arbeitgeber, Beschäftigtendaten verarbeiten zu dürfen, durch das Recht der Beschäftigten auf informationelle Selbstbestimmung begrenzt. Nach diesem darf grundsätzlich jede Person selbst über die Verarbeitung ihrer personenbezogenen Daten bestimmen.

Abwägung zwischen Rechten der Arbeitgeber/-innen und der Beschäftigten nötig

Bei der Prüfung, ob die Verarbeitung von Beschäftigtendaten für die Gestaltung von Arbeitsabläufen erforderlich ist, ist deshalb im Einzelfall eine Abwägung zwischen den Rechten der Arbeitgeberinnen und Arbeitgeber sowie der Beschäftigten vorzunehmen: Dazu müssen die Interessen der Arbeitgeberinnen und Arbeitgeber an der Datenverarbeitung und das Recht der Beschäftigten auf informationelle Selbstbestimmung zu einem Ausgleich gebracht werden, der beide Interessen möglichst weitgehend berücksichtigt.

Situation bei der Amazon Logistik Winsen GmbH

Beschäftigte dürfen nicht ununterbrochen kontrolliert werden

Um online bestellte Waren an Kundinnen und Kunden zu zugesagten Terminen liefern zu können, erhebt und nutzt die Amazon Logistik Winsen GmbH ununterbrochen Beschäftigtendaten. Dies führt dabei auch zu einer ununterbrochenen Leistungs- und Verhaltenskontrolle der Beschäftigten, was grundsätzlich rechtswidrig ist. Zudem führt eine ununterbrochene Leistungs- und Verhaltenskontrolle von Beschäftigten zu einem ständigen Überwachungs- und daran anknüpfend zu einem Anpassungs- und Leistungsdruck in allen wesentlichen Arbeitsbereichen. Dies stellt einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten dar, der grundsätzlich nicht durch von Arbeitgeberinnen und Arbeitgebern verfolgte Interessen gerechtfertigt sein kann[1].

So ist es auch hier: Die durch die Amazon Logistik Winsen GmbH mit der ununterbrochenen Erhebung und Verwendung von Beschäftigtendaten beabsichtigte pünktliche Warenlieferung sowie ihre weiteren Interessen rechtfertigen diesen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten nicht. Deshalb vertrete ich in diesem Fall die Rechtsauffassung, dass das Recht der Beschäftigten auf informationelle Selbstbestimmung das Interesse der Amazon Logistik Winsen GmbH an einer pünktlichen Warenauslieferung überwiegt. Zudem könnte die pünktliche Lieferung auch mit der Verarbeitung von weniger Beschäftigtendaten gewährleistet werden. So hielte ich es zum Beispiel für denkbar, dass ausschließlich der Standort der Ware innerhalb des Logistikzentrums verfolgt wird – ohne die Verwendung personenbezogener Daten.

Ich habe deshalb der Amazon Logistik Winsen GmbH die ununterbrochene Erhebung und Verwendung von bestimmten Beschäftigtendaten untersagt (Artikel 58 Absatz 2 Buchstabe f DS-GVO). Hiergegen hat das Unternehmen Klage vor dem zuständigen Verwaltungsgericht erhoben. Das Klageverfahren war bei Redaktionsschluss noch nicht abgeschlossen.

1 Bundesarbeitsgericht, Beschluss vom 25. April 04.2017, Az. l ABR 46/15

J.7. Gesundheit und Soziales

7.1 Fortsetzung der anlassunabhängigen Krankenhausprüfung

Eine erste, stichprobenartige Krankenhausprüfung in den Jahren 2018 und 2019 brachte die Erkenntnis, dass die Umsetzung der Vorgaben der Datenschutz-Grundverordnung (DS-GVO) bei den Verantwortlichen bereits weit fortgeschritten war. Ich möchte aber einen umfassenderen Überblick über die datenschutzrechtlichen Strukturen der Krankenhäuser in Niedersachsen erhalten, mögliche Schwachstellen aufdecken und mit entsprechenden Hilfestellungen oder Abhilfemaßnahmen reagieren können. Deshalb habe ich 2020 damit begonnen, 30 weitere, zufällig ausgewählte Krankenhäuser zu prüfen.

Die erweiterte Prüfung der Krankenhäuser gliedert sich erneut in drei Fragenkomplexe: Allgemeines zur DS-GVO und Datenschutzbeauftragten, Umgang mit der Orientierungshilfe Krankenhausinformationssysteme sowie der Komplex der Betroffenenrechte.

DS-GVO und Datenschutzbeauftragte

Datenschutzbeauftragte benötigen ausreichend Zeit

Datenschutzbeauftragte in Krankenhäusern müssen viele verschiedene datenschutzrechtliche Handlungsfelder bearbeiten. Das hat sich sowohl aus meiner letzten Krankenhausprüfung als auch aus der täglichen Arbeit meiner Behörde in diesem Bereich ergeben. Es ist jedoch fraglich, ob diese Aufgabenfülle mit dem hierfür zur Verfügung gestellten Zeitanteil überhaupt leistbar ist. Die erneute Prüfung soll zeigen, ob es in diesem Bereich Handlungsbedarf für mich als Aufsichtsbehörde gibt.

Weitere Schwerpunkte in diesem Prüfkomplex befassen sich mit dem Verzeichnis der Verarbeitungstätigkeiten und dem Prozess zur Meldung von Datenschutzverletzungen. Die tägliche Arbeit im Berichtszeitraum hat gezeigt, dass es in diesen Bereichen noch Verbesserungspotenzial gibt.

Orientierungshilfe Krankenhausinformationssysteme

Orientierungshilfe: https://t1p.de/OH-KIS

Die datenschutzrechtlichen Ausführungen der bereits in meinen vorherigen Berichten genannten Orientierungshilfe Krankenhausinformationssysteme finden weiterhin Anwendung. Ein Kernpunkt dieses Prüfkomplexes ist das Rechte- und Rollenkonzept mit den Zugriffsberechtigungen der Beschäftigten.

Betroffenenrechte

Beschwerden zum Recht auf Auskunft und Kopie

Die Einhaltung der Betroffenenrechte ist nahezu der einzige Bereich, in welchem die betroffenen Patientinnen und Patienten etwas von der Verarbeitung ihrer Daten im Krankenhaus bemerken. Ein Schwerpunkt der Beschwerden im Berichtszeitraum betraf die Umsetzung des Betroffenenrechts auf Auskunft und auf Kopie.

Die DS-GVO regelt eindeutig, dass eine Kopie der personenbezogenen Daten, welche vom Verantwortlichen verarbeitet werden, kostenfrei bereit zu stellen sind[1]. Dennoch versuchen einige Verantwortliche sich auf die zivilrechtlichen Regelungen des Patientenrechtegesetzes[2] zu beziehen und verlangen eine Aufwandsentschädigung von den Betroffenen.
Das Landgericht Dresden[3] hat hierzu mit Urteil vom 29. Mai 2020 festgestellt, dass ein Vorrangverhältnis des Patientenrechtegesetzes nicht besteht und die Auskunft unentgeltlich durch Übermittlung der vollständigen Behandlungsdokumentation erteilt werden muss.

Meine Rechtsauffassung wird durch dieses Urteil vollumfänglich bestätigt. Die Umsetzung des Auskunftsrechts nach der DS-GVO ist daher ein Kernpunkt dieses Prüfkomplexes.

Pandemiebedingte Verzögerungen berücksichtigt

Es war zu vermuten, dass auch der Bereich der Krankenhausverwaltung im Jahr der Corona-Pandemie stärker belastet war. Aus diesem Grund wurde den Verantwortlichen eine mehrmonatige Frist zur Beantwortung der Fragen gesetzt, welche erst im Jahr 2021 abläuft. Das Ergebnis dieser Prüfung werde ich daher im nächsten Tätigkeitsbericht vorstellen.

1 Art. 15 Abs. 1 und 3 DS-GVO i.V.m. Art. 12 Abs. 5 DS-GVO
2 § 630g BGB
3 Az.: 6 O 76/20, Urteil vom 29.05.2020

7.2 Patientendaten-Schutz-Gesetz – das Dilemma der elektronischen Patientenakte

Nachdem die Entwicklung einer elektronischen Patientenakte (ePA) gut 16 Jahre in Anspruch genommen hatte, hatte es der Gesetzgeber im Berichtsjahr auf einmal sehr eilig. Am 20. Oktober 2020 trat das Patientendaten-Schutz-Gesetz (PDSG) in Kraft– zum Nachteil der Krankenkassen und des Rechts auf informationelle Selbstbestimmung der Versicherten.

Ein kurzer Rückblick: Bereits im November 2003 schrieb das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung die Einführung der elektronischen Gesundheitskarte zum 1. Januar 2006 fest. Für deren Einführung und Weiterentwicklung gründeten die Spitzenverbände der Selbstverwaltung im Januar 2005 die Betriebsorganisation gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), an der inzwischen das Bundesgesundheitsministerium 51 Prozent der Anteile hält.

Anschluss der Arztpraxen an die Telematik

Die Einführung der elektronischen Gesundheitskarte verzögerte sich jedoch deutlich. Die Ausgabe der Karte durch die Krankenkassen begann erst im Oktober 2011. Seit Januar 2014 wurde schließlich die traditionelle Krankenversicherungskarte bundesweit durch die elektronische Gesundheitskarte, nun mit Lichtbild des Versicherten, abgelöst.

Versicherte sollen Zugriff auf Behandlungsdaten haben

Das „E-Health-Gesetz“ von 2015 legte dann den Grundstein zur Einführung einer elektronischen Patientenakte und eines elektronischen Patientenfachs (ePF). Ziel sollte es sein, dass Versicherte ständigen Zugriff auf ihre Behandlungsdaten haben und diese somit Ärztinnen und Ärzten sowie Therapeutinnen und Therapeuten praxisübergreifend zur Verfügung stellen können. Die gematik war nach § 291a Absatz 5c des E-Health-Gesetzes verpflichtet, bis zum 31. Dezember 2018 die erforderlichen technischen und organisatorischen Verfahren für eine fall- und einrichtungsübergreifende Dokumentation zu erarbeiten.

Nachdem die technischen Standards weitgehend feststanden, folgte die Anbindung der niedergelassenen Arztpraxen an das gesicherte Netz der Telematik-Infrastruktur (TI). Durch das Digitale Versorgungsgesetz (DVG) wurden neben den Arztpraxen und Krankenhäusern auch die Apotheken zur Anbindung an die TI bis Ende 2020 verpflichtet.

Start der elektronischen Patientenakte

Ab Januar 2021 sollen nun die Versicherten erstmalig, wenn auch mit Einschränkungen, die Möglichkeit erhalten, ihre Patientenakte elektronisch zu verwalten. Nach dem im Oktober in Kraft getretenen PDSG ist es den Patientinnen und

Patienten überlassen, ob und welche ihrer Daten sie in die elektronische Patientenakte übertragen und welche Ärztinnen und Ärzte ebenfalls Daten einstellen und auf Daten zugreifen dürfen.

Neben Befunden, Arztberichten oder Röntgenaufnahmen sollen ab 2022 auch der Impfausweis, der Mutterpass, das gelbe Untersuchungsheft für Kinder oder das Zahn-Bonusheft in die ePA aufgenommen werden können.

Unzureichendes Berechtigungskonzept

Start der elektronischen Patientenakte kommt zu früh

Leider wurde der Startzeitpunkt der ePA durch den Gesetzgeber mit dem 1. Januar 2021 deutlich zu früh gewählt. Dies ist besonders ärgerlich, da der Gesetzgeber Kenntnis davon hatte, dass die gematik, die Krankenkassen und die weiteren an der Entwicklung beteiligten Stellen frühestens zum 1. Januar 2022 in der Lage sein werden, ein feingranulares Zugriffs- und Berechtigungsmanagement technisch umzusetzen, mit dem Versicherte im Detail entscheiden können, welcher Arzt welche Befunde sehen darf.

Stattdessen wurde eine Regelung in das Gesetz aufgenommen, wonach es im Jahr 2021 ausreichen soll, dass den Versicherten nur ein grobgranulares Berechtigungskonzept zur Verfügung gestellt wird. Wenn Versicherte die ePA nutzen und mit ihren Ärztinnen und Ärzten Daten austauschen möchten, haben sie in diesem Jahr nur die Möglichkeit, alle gespeicherten Daten jedem Behandelnden zu offenbaren. So kann die Orthopädin die medizinischen Befunde des Gynäkologen oder des Psychiaters lesen. Mit dieser eingeschränkten Funktionalität verstößt die ePA gegen die mit der Datenschutz-Grundverordnung (DS-GVO) garantierten Rechte der Betroffenen hinsichtlich der Erforderlichkeit und der Zweckbindung[1] bei der Verarbeitung der sensiblen Gesundheitsdaten.

Einschränkung der Patientensouveränität

Für die Verwaltung der ePA durch die Betroffenen ist die Nutzung eines geeigneten Geräts (Smartphone, PC usw.) erforderlich. Dies ist bei einer elektronisch geführten Patientenakte nicht ungewöhnlich. Laut Gesetz soll die ePA jedoch auch Personen zur Verfügung stehen, die keine eigenen Geräte haben oder nutzen wollen (sogenannte Frontend-Nicht-Nutzer). Im ersten Referentenentwurf hatte der Gesetzgeber die Krankenkassen noch verpflichtet, in ihren Niederlassungen entsprechende Geräte bereitzustellen, welche es den Frontend-Nicht-Nutzern unter Wahrung des Rechts auf informationelle Selbstbestimmung ermöglichen sollten, ihre ePA zu verwalten. Im weiteren Gesetzgebungsverfahren wurde diese Verpflichtung leider gestrichen.

Stattdessen hat der Gesetzgeber ab dem Jahr 2022 vorgesehen, dass diese Personen einen Dritten mit der Verwaltung ihrer Daten oder mit der Wahrnehmung des Rechts auf Auskunft[2] über die in der ePA gespeicherten Daten beauftragen können. In diesem Fall ist es unumgänglich, dass der Dritte Kenntnis von den sensiblen Gesundheitsdaten der betroffenen Person erhält. Aus datenschutzrechtlicher Sicht stellt dies eine unzulässige Einschränkung der Patientensouveränität hinsichtlich der datenschutzrechtlichen Grundsätze der Integrität, Vertraulichkeit und Verfügbarkeit[3] dar.

1 Art. 5 Abs. 1 Buchst. b) DS-GVO

2 Art. 15 DS-GVO

3 Art. 5 Abs. 1 Buchst, f) DS-GVO, Art. 32 Abs. 1 Buchst, b) DS-GVO

Würden die Krankenkassen verpflichtet, den Frontend-Nicht-Nutzern Terminals für die Nutzung der ePA bereit zu stellen, wäre der Datenschutz für alle Nutzenden gewahrt.

Dilemma auch für die Krankenkassen

Obwohl die technische Umsetzung der ePA noch nicht abgeschlossen ist, verpflichtet das PDSG die gesetzlichen Krankenkassen, den Versicherten im Jahr 2021 eine ePA anzubieten. Die Krankenkassen als Verantwortliche für die ePA wurden so in die missliche Situation gezwungen, entweder die Vorgaben des PDSG zu erfüllen, indem sie die elektronische Patientenakte ab Januar 2021 anbieten, oder die Vorgaben der DS-GVO einzuhalten. Beides gleichzeitig zu schaffen, ist zumindest 2021 nicht möglich.

2021 gilt: Entweder PDSG oder DS-GVO

Eine Verschiebung des Beginns der ePA auf das Jahr 2022 wäre die einzige Möglichkeit gewesen, die Krankenkassen nicht in das beschriebene Dilemma zu bringen.

Intervention der Datenschutzbeauftragten

Nach Bekanntwerden des vom Bundestag verabschiedeten Gesetzentwurfs habe ich gemeinsam mit Kolleginnen und Kollegen aus Bund und Ländern am 19. August 2020 im Rahmen der Bundespressekonferenz auf die datenschutzrechtlichen Missstände hingewiesen. Zusätzlich habe ich mit Schreiben vom 27. August 2020 das Niedersächsische Ministerium für Soziales, Gesundheit und Gleichstellung, die Niedersächsische Staatskanzlei und die im Niedersächsischen Landtag vertretenen Fraktionen informiert und aufgefordert, vor der Verabschiedung des PDSG im Bundesrat dort auf die Anrufung des Vermittlungsausschusses hinzuwirken und in Bezug auf den Datenschutz im Jahr 2021 nachzubessern.

Am 1. September 2020 machte die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) im Rahmen einer Entschließung ebenfalls auf die datenschutzrechtlichen Missstände aufmerksam.

Entschließungen der DSK: https://t1p.de/dsk-entschliessungen

Dennoch verzichtete der Bundesrat in seiner Sitzung am 18. September 2020 auf eine Anrufung des Vermittlungsausschusses und billigte das PDSG in der vom Bundestag beschlossenen Fassung[4]. Das PDSG trat am 20. Oktober 2020 ohne Berücksichtigung der von den Datenschutzaufsichtsbehörden geforderten Änderung in Kraft.

Aufsichtsbehördliche Maßnahme ergriffen

Als letztes Mittel blieb mir daher nur die Möglichkeit, eine Warnung gegenüber der in meinem Zuständigkeitsbereich befindlichen gesetzlichen Krankenkasse auszusprechen. Dies habe ich am 23. November 2020 getan und davor gewarnt, lediglich die im PDSG enthaltenen Vorgaben zur technischen Ausgestaltung der ePA einzuhalten sowie auf ein feingranulares Zugriffsmanagement bei der Einführung der ePA zu verzichten. Die Krankenasse hat mit daraufhin mitgeteilt, dass sie meine Bedenken teilt, hat aber zugleich auf ihre Verpflichtung zur Einhaltung der gesetzlichen Vorgaben im PDSG verwiesen.

4 BT-Drs. 19/18793, 19/20708

7.3 Entbindung vom Bankgeheimnis im Rahmen der Gewährung von Sozialhilfe

Wer Sozialleistungen beantragt oder erhält, ist dazu verpflichtet, Beweismittel, die für die Leistung erheblich sind, auf Verlangen des zuständigen Leistungsträgers vorzulegen. Der Leistungsträger darf aber keine Entbindung vom Bankgeheimnis verlangen.

Einer Beschwerdeführerin wurden Leistungen nach dem Sozialgesetzbuch (SGB) XII versagt. Sie war im Rahmen der Überprüfung ihrer wirtschaftlichen Verhältnisse aus folgenden Gründen nicht bereit, dem für sie zuständigen Leistungsträger eine Entbindung vom Bankgeheimnis zu erteilen:

- der Leistungsträger hatte die Entbindung vom Bankgeheimnis bereits unmittelbar mit der Aushändigung der Antragsunterlagen angefordert;
- unter der Androhung, dass ohne diese der Antrag wegen fehlender Mitwirkung abgelehnt wird;
- ohne dass konkrete Verdachtsmomente für einen Sozialleistungsbetrug vorlagen;
- obgleich dem Leistungsträger im Rahmen der Antragsstellung u. a. lückenlos sämtliche Kontoauszüge sämtlicher bestehender Bankkonten (Giro- und Sparkonto) der vergangenen drei Monate vor Antragsstellung eingereicht wurden;
- ungeachtet der ohnehin bestehenden gesetzlichen Grundlage für einen Kontenabruf[1].

Bei seiner ablehnenden Entscheidung berief sich der Leistungsträger darauf, dass er einer verbindlichen Vorgabe des örtlichen Sozialhilfeträgers, in dessen Auftrag er Leistungen der Sozialhilfe ausführt, zu folgen habe.

Mitwirkungspflicht der antragsstellenden Person

Wer Sozialleistungen beantragt oder erhält, ist u. a. dazu verpflichtet, Beweismittel[2], die für die Leistung erheblich sind, auf Verlangen des zuständigen Leistungsträgers vorzulegen oder der Vorlage durch Dritte zuzustimmen[3]. Wird dieser Mitwirkungspflicht nicht nachgekommen und wird hierdurch dem Leistungsträger die Aufklärung erheblich erschwert, ob die Voraussetzungen für einen Leistungsbezug vorliegen, kann der Leistungsträger ohne weitere Ermittlungen die Leistung bis auf weiteres entziehen[4].

Ohne Mitwirkung können Leistungen entzogen werden

1 § 93 Abs. 8 Abgabenordnung (AO)

2 § 21 SGB X

3 § 37 SGB I in Verbindung mit (i. V. m.) § 60 Abs. 1 Nr. 3 SGB I

4 § 37 SGB I i. V. m. § 68 Abs. 1 Satz 1 SGB I

Allerdings darf eine Mitwirkung nur soweit verlangt werden, als sie zur Aufklärung eines Sachverhalts erforderlich ist. So hat ein Leistungsträger der antragstellenden Person zunächst Gelegenheit zu geben, selbst die für den Leistungsbezug erforderlichen Auskünfte zu erteilen und entsprechende Nachweise (z. B. Kontoauszüge) vorzulegen. Antragstellende Personen kommen im Rahmen der Überprüfung ihrer wirtschaftlichen Verhältnisses ihrer Mitwirkungspflicht regelmäßig vollumfänglich nach, sofern sie einem Leistungsträger vollständige Auszüge der letzten drei Monate vor Antragstellung aller ihrer bestehenden Konten vorlegen.

Entbindung vom Bankgeheimnis

Kein Allgemeinverdacht gegen Bedürftige

Ein diffuses Misstrauen gegenüber bedürftigen Personen und ein darauf gestützter Allgemeinverdacht, dass sich diese durch unrichtige oder unvollständige Angaben Leistungen erschleichen wollen, rechtfertigt nicht, eine Entbindung vom Bankgeheimnis zu verlangen. Dies gilt insbesondere, da sich mithilfe einer Entbindung vom Bankgeheimnis nicht aufklären lässt, ob die antragstellende Person vollständige Angaben zu ihren bestehenden Bankkonten gemacht hat oder nicht.

Sofern ein begründeter Verdacht für einen möglichen Sozialleistungsmissbrauch besteht, sind die zuständigen Behörden, nach § 93 Abs. 8 Nr. 1 b) AO berechtigt, ein Kontenabrufersuchen beim Bundeszentralamt für Steuern zu stellen. Zumindest wenn dies zur Überprüfung der Anspruchsvoraussetzungen erforderlich ist und ein vorheriges Auskunftsersuchen bei der antragstellenden Person nicht zum Ziel geführt hat.

Ferner sind diejenigen, die für einen Hilfebedürftigen Guthaben führen oder Vermögensgegenstände verwalten (also in erster Linie Geld- oder Kreditinstitute sowie Versicherungen), nach § 117 Abs. 3 SGB XII dazu verpflichtet, einem Träger der Sozialhilfe auf dessen Verlangen hierüber Auskunft zu erteilen.

Ergebnis meines Kontrollverfahrens

Der Leistungsträger nahm nach meiner Intervention seine ablehnende Entscheidung zurück und gewährte der Beschwerdeführerin die von ihr beantragten Leistungen nach dem SGB XII.
Die für den Leistungsträger zuständige Region Hannover wies sämtliche Kommunen, die Leistungen der Sozialhilfe in ihrem Auftrag ausführen, an, zukünftig eine Entbindung vom Bankgehemins nicht mehr verpflichtend zu verlangen.

J.8. Telemedien

8.1 Prüfung zum Tracking auf Webseiten 15 niedersächsischer Unternehmen

Niedersächsische kleine und mittelständische Unternehmen setzen auf ihren Firmen-Webseiten Cookies und Drittdienste eher sparsam ein, informieren aber zugleich die Nutzerinnen und Nutzer zu wenig darüber, welche Daten beim Besuch ihrer Seiten erhoben werden. Das geht aus einer branchenübergreifenden Prüfung hervor, die ich zum datenschutzkonformen Tracking auf Webseiten durchgeführt habe.

Pressemitteilung zur Prüfung: https://t1p.de/pm-tracking

Das Thema datenschutzkonformes Tracking auf Webseiten erfährt seit der Geltung der Datenschutz-Grundverordnung (DS-GVO) wieder erhöhte Aufmerksamkeit. Nach den Entscheidungen des Europäischen Gerichtshofs (EuGH) 2019 und des Bundesgerichtshofs (BGH) 2020 zum Verfahren Planet 49 (siehe F.3, S. 57) war eine deutliche Entwicklung in diesem Bereich zu beobachten. Vermutlich hat jeder Internetnutzer und jede Internetnutzerin gemerkt, dass sich auf zahlreichen Webseiten die sogenannten Consent-Fenster stark verändert haben. Diese enthalten immer häufiger mehr Informationen und mehr Auswahlmöglichkeiten sowie im besten Fall eine echte Entscheidungsfreiheit für Nutzerinnen und Nutzer. Diese Entwicklung ist aus datenschutzrechtlicher Perspektive eine deutliche Verbesserung.

Prüfungsablauf: Fragebogen und technische Kontrolle

Vor diesem Hintergrund führte ich in Niedersachsen eine branchenübergreifende Prüfung von 15 kleinen und mittelständischen Unternehmen durch. Diese wurden schriftlich gebeten, einen umfassenden Fragebogen zu beantworten. Die Unternehmen sollten unter anderem beantworten, ob sie Dienste von Drittanbietern (z.B. Karten- oder Wetterdienste) eingebunden hatten, ob sie Cookies einsetzten und ob sie deren Verwendung auf eine Einwilligung der Nutzerinnen und Nutzer stützten.

Zusätzlich wurden insgesamt 22 Webseiten der Unternehmen technisch überprüft – sowohl vor als auch nach der Versendung der Fragebögen. Der Auswertung wurden die ausgefüllten Fragebögen, die Ergebnisse der technischen Prüfungen und die auf den Webseiten verfügbaren Datenschutzerklärungen zugrunde gelegt.

Bewertete Kriterien

Im Einzelnen wurden die folgenden Kriterien bewertet:

1. Rechtmäßigkeit der Datenverarbeitung im Zusammenhang mit Cookies und Drittdiensten
2. Wirksamkeit der Einwilligung, sofern eine Einwilligung auf der Webseite für die Verarbeitung von Cookies oder die Einbindung von Drittdiensten eingeholt wird
3. Erfüllung der Informationspflichten gemäß Art. 13 DS-GVO

Zu diesen drei Themen erfolgte eine Ampelbewertung. Grün, wenn die Webseite den Anforderungen der DS-GVO entsprach. Gelb, wenn, in Bezug auf einige Anforderungen Defizite festgestellt wurden, die mit geringem Aufwand behoben werden können. Rot, wenn erhebliche Defizite festgestellt wurden. Aus den drei Einzelbewertungen ergab sich eine Gesamtbewertung, ebenfalls nach dem Ampelprinzip.

Wesentliche Ergebnisse

1. Rechtmäßigkeit der Datenverarbeitung im Zusammenhang mit Cookies und Drittdiensten

Für 16 Webseiten (73 %) gaben die Befragten an, Dienste von Dritten eingebunden zu haben. In die Bewertung wurden alle Drittdienste einbezogen, unabhängig davon, ob die Einbindung über ein Cookie oder andere technische Mechanismen erfolgte.

Eingebundene Drittdienste

Die folgenden Dienste wurden genannt:

- Analyse- und Tracking-Dienste: Google Analytics, eTracker, Wiredminds.
- Marketingdienste: Google Dynamic Remarketing, Google AdWords
- Kartendienste: Google Maps, Open-Street-Map
- Chatdienst: Chatsuite
- Consent-Tool: Cookiebot
- Weitere: Google Tag Manager, Google Fonts, YouTube, Wordpress.

Die technische Prüfung ergab, dass auf allen Webseiten Cookies eingesetzt wurden – allerdings jeweils nur in recht geringer Anzahl von einem bis 14 Cookies. Auf sieben Webseiten wurden ausschließlich eigene Cookies und keine von Drittdienstleistern eingesetzt.

Es entstand der Eindruck, dass sich die Mehrheit der Webseitenbetreiber bewusst mit dem Einsatz von Cookies auseinandergesetzt hatte. Deren datenschutzrechtliche Relevanz ist weitgehend bekannt. Zumindest auf explizite Nachfrage machte die Mehrheit Angaben zur Rechtsgrundlage der Verarbeitung. Es wurde im Wesentlichen auf Art. 6 Abs. 1 lit. a (Einwilligung der Betroffenen), lit. b (Erfüllung eines Vertrages) oder lit. f (berechtigtes Interesse des Verantwortlichen und Interessenabwägung) DS-GVO abgestellt.

Unsicherheiten bei der Prüfung der Rechtsgrundlagen

Knapp die Hälfte der Befragten (7 von 15) schätzten die Rechtsgrundlage für die eingesetzten Cookies korrekt ein. Der häufigste Wertungsfehler lag in der Abgrenzung zwischen den Anwendungsbereichen von Art. 6 Abs. 1 lit. f DS-GVO (berechtigtes Interesse des Verantwortlichen

und Interessenabwägung) und Art. 6 Abs. 1 lit. a DS-GVO (Einwilligung der betroffenen Person). Das heißt, der Einsatz von Cookies, die von den Aufsichtsbehörden als einwilligungsbedürftig eingestuft wurden, wurden von einigen Verantwortlichen auf die Wahrung ihrer berechtigten Interessen gestützt. Allerdings wurde dann nicht immer deutlich, dass eine Abwägung zwischen den Interessen der Betroffenen und denen der Verantwortlichen vorgenommen worden war. Einige Verantwortliche nahmen sehr pauschal ein eigenes berechtigtes Interesse an, ohne auf die Interessen und Rechte der betroffenen Personen einzugehen.

2. Wirksamkeit der Einwilligung

Auf drei Webseiten wurden keine Einwilligungen eingeholt und waren auch nicht erforderlich. Auf den übrigen 19 Webseiten fand sich mindestens ein Cookie-Hinweis. Um die Wirksamkeit der eingeholten Einwilligung zu prüfen, wurden sieben Anforderungen bewertet:

Anforderungen an die Einwilligung

- Zeitpunkt der Einwilligung
- Informiertheit der Einwilligung
- Eindeutige bestätigende Handlung
- Freiwillige Einwilligung
- Kein unzulässiges Nudging
- Nachteile bei Verweigerung der Einwilligung
- Widerruf der Einwilligung

Nur auf einer der 19 Webseiten, die Einwilligungen einholten, war diese wirksam. Bei der überwiegenden Zahl der geprüften Seiten war die Einwilligung aufgrund erheblicher Mängel unwirksam.

Erhebliche Defizite waren bei der Bereitstellung von Informationen im ersten Fenster des Consent-Tools festzustellen. Lediglich ein Verantwortlicher erteilte die Mindestinformationen nahezu vollständig und korrekt. Bei allen anderen Verantwortlichen wurden teils erhebliche Informationsdefizite in Bezug auf die informierte Einwilligung festgestellt.

Nudging als Mittel zur Einwilligung

Mehrere Verantwortliche setzten auf ihren Webseiten Nudging ein. Damit soll das Nutzerverhalten durch subtile Eingriffe des Verantwortlichen im eigenen Interesse unterschwellig beeinflusst werden. Häufig ist etwa die „Zustimmen"-Option im Vergleich zur „Ablehnen"-Option farblich auffälliger. Oder der Prozess des Ablehnens ist unnötig kompliziert und erfordert mehr Klicks. Bei vier Seitenbetreibern ging das Nudging in der Cookie-Einwilligung so weit, dass die damit eingeholte Einwilligung als unwirksam bewertet wurde.

3. Erfüllung der Informationspflichten gemäß Art. 13 DS-GVO

Allen 15 Befragten war die Informationspflicht bekannt, entsprechend waren auf allen Webseiten Datenschutzerklärungen verfügbar. Die formalen Anforderungen gemäß Art. 12 DS-GVO wurden von der überwiegenden Zahl der Verantwortlichen erfüllt, allerdings fanden sich in einigen Datenschutzklärungen teils widersprüchliche Aussagen.

Informationen häufig nicht vollständig oder korrekt

Teils erhebliche Defizite bestanden beim gesetzlich vorgegebenen Informationsumfang. Lediglich auf drei der geprüften Webseiten wurden alle gemäß Art. 13 DS-GVO erforderlichen Informationen gegeben. Bei den restlichen Seiten fehlten insbesondere differenzierte Angaben zu den Rechtsgrundlagen sowie zur Speicherdauer von Cookies.

Fazit und Ausblick

In der Gesamtschau kann ich die Prüfung nur als positiv bewerten. Die festgestellten Defizite waren überschaubar und die meisten Verantwortlichen nahmen umgehend Verbesserungen auf ihren Webseiten vor. Meine Behörde hat wertvolle Erkenntnisse gewonnen, welche datenschutzrechtlichen Standardfehler in diesem Bereich vorherrschen. Diese wurden in der anschließend erstellten und veröffentlichten Handreichung mit Hinweisen für die Ausgestaltung von Einwilligungen auf Webseiten aufgegriffen, so dass ich hier weiteres Informationsmaterial mit konkretem Praxisbezug zur Verfügung stellen konnte.

Hinweise für die Anforderungen an Consent-Layer: https://t1p.de/consent-layer

Dennoch ist mir sehr bewusst, dass die Ergebnisse dieser branchenübergreifenden Prüfung nicht für alle Wirtschaftsbereiche in der Tiefe repräsentativ sein können. Unter den geprüften Unternehmen fanden sich keine, deren Webseiten ein wesentlicher Teil ihres Geschäftsmodell ist oder die ausschließlich im Online-Bereich tätig sind. Daher führe ich momentan mit den Aufsichtsbehörden mehrerer anderer Bundesländer eine koordinierte Prüfung der Webseiten von Online-Medien durch. Die endgültigen Ergebnisse hierzu liegen noch nicht vor. Aber bereits jetzt lässt sich feststellen, dass erwartungsgemäß auf den Webseiten der Medienhäuser eine erheblich größere Anzahl von Cookies und Drittdiensten eingebunden ist als auf den Seiten der in der beschriebenen Prüfung vertretenen Unternehmen.

J.9. Videoüberwachung

9.1 Polizeiliche Videobeobachtung in Hannover rechtswidrig

Auf Grundlage des Niedersächsischen Polizei- und Ordnungsbehördengesetzes besteht für die Polizei die Möglichkeit, öffentliche Straßen und Plätze mit Videotechnik zu überwachen und die übertragenen Bilder aufzeichnen[1]. Dass hierbei stets die entsprechenden Tatbestandsvoraussetzungen zu erfüllen sind, zeigt ein im Berichtszeitraum ergangenes Urteil des Niedersächsischen Oberverwaltungsgerichts vom 6. Oktober 2020[2].

Der 11. Senat des Niedersächsischen Oberverwaltungsgerichts entschied, dass die von der Polizeidirektion (PD) Hannover betriebenen Veranstaltungskameras an den Standorten Rudolf-von-Bennigsen-Ufer, Bruchmeisterallee, Lister Platz, Schützenplatz und TUI-Arena zum Zeitpunkt der gerichtlichen Feststellung rechtswidrig waren. Auch die Videoüberwachung an den Standorten Königsworther Platz und Theodor-Heuss-Platz, an denen die Kamers im März 2020 demontiert worden waren, wurden dort bis zum Zeitpunkt der Demontage rechtswidrig betrieben.

VG Hannover gibt Klage gegen Kameras statt

Der Kläger hatte sich gegen die von der PD in Hannover an verschiedenen öffentlich zugänglichen Orten betriebene Videoüberwachung gewandt. Mit Urteil vom 9. Juni 2016[3] hatte das Verwaltungsgericht Hannover seiner ursprünglich auf 78 Kameras bezogenen Klage in Bezug auf 56 Kamerastandorte stattgegeben und der PD Hannover aufgegeben, an diesen Standorten die Bildübertragung sowie die Aufzeichnung zu unterlassen. Hinsichtlich der weiteren 22 Standorte hatte es die Klage abgewiesen, da diesbezüglich die Voraussetzungen nach dem – zum Zeitpunkt des Urteilserlasses geltenden – Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung für eine Videobeobachtung und Aufzeichnung vorgelegen hätten.

1 § 32 Absatz 3 NPOG

2 Aktenzeichen 11 LC 149/16

3 Aktenzeichen 10 A 4629/11

PD Hannover legt Berufung ein

Mit ihrer gegen dieses Urteil eingelegten Berufung beantragte die PD Hannover ursprünglich, das Urteil des Verwaltungsgerichts abzuändern, soweit es der Klage stattgegeben hatte, und die Klage in vollem Umfang abzuweisen. Im Laufe des Berufungsverfahrens stellte die Polizei aber den Betrieb von 51 der vom Verwaltungsgericht untersagten Kamerastandorte ein oder übertrug den Betrieb auf andere Behörden. In Bezug auf 49 dieser Standorte erklärten die Beteiligten das Verfahren übereinstimmend für erledigt. Hinsichtlich zweier weiterer Standorte (Königsworther Platz und Theodor-Heuss-Platz), an denen die PD seinerzeit beabsichtigte, den Betrieb der Kameras im Jahr 2021 unter Einsatz neuer Kameramodelle wiederaufzunehmen, passte der Kläger seinen Klageantrag an und beantragte festzustellen, dass der Betrieb dieser Kameras rechtswidrig war.

Zu den Kamerastandorten, für welche die Beteiligten übereinstimmende Erledigungserklärungen abgegeben hatten, stellte der Senat das Verfahren ein. Hinsichtlich der fünf aktuell noch von der PD betriebenen Veranstaltungskameras an den Standorten Rudolf-von-Bennigsen-Ufer, Bruchmeisterallee, Lister Platz, Schützenplatz und TUI-Arena hatte die Berufung keinen Erfolg, da der Betrieb dieser Standorte zum Zeitpunkt der gerichtlichen Entscheidung rechtswidrig war. In Bezug auf die Kamerastandorte Königsworther Platz und Theodor-Heuss-Platz stellte der Senat fest, dass der Betrieb dieser Kameras bis zur Demontage im März 2020 rechtswidrig war.

Übersicht über polizeiliche Kamerastandorte in Hannover
https://t1p.de/pol-kameras

Begründung des Oberverwaltungsgerichts

Zur Begründung führte der Senat aus, dass die Videobeobachtung zwar einen Eingriff in das Recht auf informationelle Selbstbestimmung darstelle, der jedoch grundsätzlich durch die nunmehr seit dem 24. Mai 2019 gültigen § 32 Absatz 3 Satz 1 Nummer 1 und Nummer 2 in Verbindung mit Satz 2 und Satz 3 NPOG gerechtfertigt werden könne. Die PD habe jedoch nicht ausreichend dargelegt, dass die tatbestandlichen Voraussetzungen dieser Normen erfüllt seien. So entspreche die von der PD vorgenommene Kenntlichmachung nicht den Anforderungen des § 32 Absatz 3 Satz 2 NPOG. Die auf vorhandenen Pfosten angebrachten Aufkleber seien aufgrund der Krümmung der Pfosten und der Vielzahl der regelmäßig darauf angebrachten anderen Aufkleber und Hinweiszettel für den durchschnittlichen Verkehrsteilnehmer – anders als die früher teilweise genutzten Hinweisschilder – nicht ausreichend wahrnehmbar.

Auch seien die von der PD vorgelegten Jahresstatistiken nicht geeignet, den nach § 32 Absatz 3 Satz 1 Nummer 2 NPOG erforderlichen Zusammenhang zwischen einer temporären Veranstaltung und einer im zeitlichen und örtlichen Zusammenhang mit dieser Veranstaltung zu erwartenden Straftat darzulegen. Zudem habe die PD keine Daten dazu vorgelegt, wann sie die temporär genutzten Veranstaltungskameras jeweils aktiviert habe und welche Straftaten in diesen Zeiträumen erfasst worden seien.

Statistiken der Polizei nicht geeignet

Der Senat ließ die Revision zum Bundesverwaltungsgericht nicht zu. Auch wurde keine Nichtzulassungsbeschwerde durch die PD Hannover eingereicht, so dass die Entscheidung rechtskräftig geworden ist.

Meine Reaktion

Die Polizeidirektion Hannover teilte mir auf Nachfrage mit, dass die fünf als rechtswidrig festgestellten Veranstaltungskameras noch am Tag der gerichtlichen Entscheidung in eine sogenannte

„Nullstellung“ (das Kameraobjektiv wurde in eine Position gefahren, die eine Beobachtung von Bürgerinnen und Bürgern nicht mehr möglich machte) gefahren wurden.

Am 9. Oktober 2020 wurden die Kameras zudem im Videoverbundnetz abgeschaltet, so dass ein Zugriff durch die Polizeidirektion Hannover auch technisch nicht mehr möglich war. Die Kennzeichnungen wurden durch die Polizei entfernt.

Ein technischer Abbau sei mit dem Urteil nicht gefordert worden. Vielmehr dauere in der Polizeidirektion Hannover gegenwärtig noch die Prüfung an, ob die Voraussetzungen, welche das Oberverwaltungsgericht Lüneburg in seinem Urteil an eine Wiederinbetriebnahme der temporär genutzten Veranstaltungskameras geknüpft hatte, für die jeweiligen Standorte erfüllt werden können.

Bei den übrigen 23 Standorten mit 26 Kameras, welche nicht Gegenstand des OVG-Urteils waren, wurden seit Dezember 2020 die alten Aufkleber sukzessive durch neue Hinweistafeln aus Metall in der vorgeschriebenen Größe ersetzt.
Nur in wenigen Einzelfällen werden Aufkleber verwendet, beispielsweise wenn diese auf weitgehend ebenen Flächen angebracht werden können. Das OVG Lüneburg hat insoweit nur die krümmungsbedingte eingeschränkte Erkennbarkeit an runden Pfosten, nicht aber den Inhalt der Beschilderung selbst beanstandet.

Zukünftig werde ich die Polizei auffordern, mir die Jahresstatistiken für eine Prüfung im Sinne des ergangenen Urteils zu übersenden.

9.2 Videoüberwachung in Schlachthöfen

In der Vergangenheit haben sich in Schlachthöfen in Niedersachsen und anderen Bundesländern wiederholt Verstöße gegen das Tierschutzgesetz ereignet. Häufig wurden diese Verstöße durch heimlich angefertigte Filmaufnahmen von Tierschutzorganisationen publik gemacht. Als Reaktion hierauf führten einige Schlachtbetriebe eine umfangreiche Videoüberwachung ein, um einen gesetzeskonformen Umgang mit den Tieren nachweisen zu können. Doch wie sind die Belange des Tierschutzes mit den oftmals durch die Videoüberwachung betroffenen Rechten der Beschäftigten in Einklang zu bringen?

Bereits im Februar 2019 hatte das Niedersächsische Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz (ML) eine freiwillige Vereinbarung mit mehreren Verbänden der fleischverarbeitenden Betriebe, dem Niedersächsischen Landkreistag sowie dem Niedersächsischen Städtetag zur Einführung von kameragestützten Überwachungssystemen in niedersächsischen Schlachthöfen zur Verbesserung des Tierschutzes getroffen. Demnach soll die Videoüberwachung sowohl zur Eigenkontrolle dienen als auch die amtliche Überwachung unterstützen, um im Verdachtsfall möglichen Tierschutzverstößen gezielt nachgehen zu können. Abläufe sollen dokumentiert und Prozesse verbessert werden.

Vereinbarung zur Videoüberwachung in Schlachthöfen: https://t1p.de/vereinbarung-tierschutz

Leitfaden zur Umsetzung der Vereinbarung

Aufgrund der Ausdehnung der Videoüberwachung wurden bei mir bis weit in das Jahr 2020 hinein etliche Beschwerden eingelegt, vor allem durch betroffene Beschäftigte der Schlachtbetriebe. Problematisch waren insbesondere die permanente Überwachung der Beschäftigten sowie die angestrebte mehrmonatige Speicherung der Bilddaten. Da sich Unternehmen auch immer wieder auf die mit dem ML getroffene Vereinbarung bezogen und dort um Unterstützung gegenüber der Aufsichtsbehörde nachfragten, erkannten alle Beteiligten den Bedarf an der Erarbeitung einer Handlungsempfehlung. Daher unterstützte ich das ML bei der Erstellung eines Leitfadens zur datenschutzrechtskonformen Umsetzung der 2019 getroffenen Vereinbarung.

Leitfaden: https://t1p.de/leitfaden-schlachthoefe

Zu den wichtigen Eckpunkten dieses Leitfadens gehört der Hinweis, dass der Erfassungsbereich der Kameras so zu beschränken ist, dass nur tierschutzrelevante Bereiche erfasst werden. Bereiche, in denen sich Beschäftigte regelmäßig zur Arbeitserledigung aufhalten, müssen aus der Erfassung herausgenommen, verpixelt oder unkenntlich gemacht werden.

Datenschutzrechtliche Prüfungen

Bei meinen Kontrollen der Videoüberwachung in Schlachthöfen wird jede Kamera einer Einzelfallüberprüfung unterzogen. Rechtsgrundlage für die Über-

wachung ist Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DS-GVO). Demnach ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen der Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Keine dauerhafte Überwachung von Beschäftigten

Lediglich der begründete Verdacht auf eine konkrete Straftat kann nach § 26 Absatz 1 Satz 2 des Bundesdatenschutzgesetzes (BDSG) ein berechtigtes Interesse an der begrenzten Überwachung einzelner Beschäftigter darstellen. Da diese Voraussetzungen in der Regel nicht oder zumindest nicht dauerhaft vorliegen, kann die dauerhafte Überwachung der Beschäftigten nicht darauf gegründet werden.

Teilweise wurde von den Betrieben geltend gemacht, dass die Überwachung Kundenanforderungen diene. Kundinnen und Kunden würden regelmäßig von den Schlachtbetrieben einen Nachweis darüber verlangen, dass bei der Schlachtung verantwortungsvoll unter Einhaltung der tierschutzrechtlichen Vorgaben gearbeitet wurde. Durch die Möglichkeit des Zugriffs auf die Videoaufzeichnungen der Schlachtbetriebe werde diese Kontrollmöglichkeit geschaffen.
Auch lange Speicherfristen wurden mit Kundenanforderungen begründet. Das kann jedoch keine Grundlage für eine Videoüberwachung oder die Festlegung der Speicherdauer sein. Den Kundinnen und Kunden steht hierfür in der Regel keine eigene Rechtsgrundlage zur Verfügung.

Speicherfristen sind zu lang

Neben der Frage der Rechtsgrundlage waren bei den meisten der geprüften Unternehmen die Speicherfristen problematisch. Da die in der Vergangenheit von Tierschutzorganisationen gezeigten Aufnahmen mehrere Monate alt waren, bestand der Wunsch nach einer mehrmonatigen Datenspeicherung, um sich im Fall von Anschuldigungen mit dem Videomaterial verteidigen und ein tierschutzgerechtes Verhalten nachweisen zu können.

Nach Artikel 17 Absatz 1 Buchstabe a DS-GVO sind die Videoaufnahmen unverzüglich zu löschen, wenn sie zur Erreichung der Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von zwei Tagen geklärt werden können. Demnach sollten die Aufnahmen – unter Berücksichtigung des Grundsatzes der „Datenminimierung" sowie des Grundsatzes der „Speicherbegrenzung" gemäß Artikel 5 Absatz 1 Buchstabe c und Buchstabe e DS-GVO – regelmäßig nach 48 Stunden gelöscht werden.

Eine längere Speicherung für die eventuell erforderliche Abwehr von Beschuldigungen kommt einer Vorratsdatenspeicherung gleich. Dieser stehen die schutzwürdigen Interessen der Beschäftigten oder anderen erfassten Personen entgegen. Je länger die Videobilddaten aufbewahrt werden, umso mehr nimmt der Eingriff in die Persönlichkeitsrechte der Betroffenen zu. Das Risiko eines unbefugten Datenzugriffs wächst mit der Dauer der Speicherung. Daher wird eine derartige

Lange Speicherdauer nur ohne Personenbezug

lange Speicherung der Bilddaten zum Zweck der Schuldbefreiung von mir nur hingenommen, wenn diese keinen Personenbezug aufweisen. Denn für den Nachweis der gesetzeskonformen Behandlung der Tiere ist der Personenbezug nicht erforderlich.

Im Übrigen weise ich darauf hin, dass eine Videoüberwachung insbesondere dann dem Tierwohl dient, wenn eine Echtzeitbeobachtung erfolgt und im Bedarfsfall dem Tier unmittelbar geholfen wird.

9.3 Videoüberwachung in Spielbanken

Das im Grundgesetz verbriefte Recht auf freie Entfaltung der Persönlichkeit beinhaltet als eines seiner Wesenskerne, dass sich Bürgerinnen und Bürger grundsätzlich beobachtungsfrei bewegen können. Dies gilt umso mehr für die Bereiche, in denen sie sich im Rahmen ihrer Freizeitgestaltung etwa zur Entspannung aufhalten. Dieses Grundrecht kann allerdings beschränkt werden, zum Beispiel für die Besucher von Spielbanken. Die gesetzlichen Vorgaben sehen eine ausgedehnte Videoüberwachung vor, von der auch die Beschäftigten der Spielbanken umfasst sind. Dabei kommt es in der praktischen Umsetzung immer wieder zu datenschutzrechtlichen Herausforderungen.

Gemäß § 10 c des Niedersächsischen Spielbankengesetzes (NSpielbG) muss der Zulassungsinhaber in Spielbanken zur Zugangskontrolle, zum Schutz vor Sachbeschädigung, zur Verhinderung, Aufdeckung und Verfolgung von Straftaten, zur Überwachung der Spielverbote nach der Spielordnung und zur Sicherung des Vertrauens der Öffentlichkeit in ein ordnungsgemäßes Spiel die folgenden Bereiche videoüberwachen:

- Eingänge,
- Bereiche, in denen üblicherweise der Transport, die Zählung oder die Aufbewahrung von Bargeld oder Spielmarken erfolgt, sowie
- die Spielräume der Spielbank und die Spieltische und Automaten.

Finanzministerium macht Vorgaben zur Videoüberwachung

Die Fachaufsicht über den Zulassungsinhaber und die von ihm betrieblichen öffentlichen Spielbanken übt gemäß § 10 NSpielbG das Niedersächsische Finanzministerium (MF) aus. Auch die Videoüberwachung in Spielbanken ist Bestandteil der Zulassungsprüfung durch die Fachaufsicht. Nach § 10 c Absatz 1 Satz 2 NSpielG können der Umfang und die einzuhaltenden technischen Anforderungen, insbesondere die aufzuzeichnenden Bildraten und die Auflösung der Videoüberwachung vom Fachministerium in der Spielbankerlaubnis oder in aufsichtsbehördlichen Anordnungen festgesetzt werden. Das bedeutet, dass die Betreiberinnen und Betreiber der Spielbanken die Videoüberwachung entsprechend der Vorgaben des MF umsetzen müssen, wenn sie die Konzession nicht verlieren wollen.

Aufsichtsrechtliches Dilemma

Gleichzeitig ist gemäß § 10 d NSpielbG der Zulassungsinhaber Verantwortlicher für die Verarbeitung personenbezogener Daten und somit für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich. Damit ist er auch Adressat etwaiger Aufsichtsmaßnahmen meiner Behörde.
Der Betreiber oder die Betreiberin einer Videoüberwachungsanlage in Spielbanken unterliegt somit in der Konsequenz der Fachaufsicht durch das MF und in datenschutzrechtlicher Hinsicht der Aufsicht durch meine Behörde.

Diese Konstellation ist in der Praxis für den Zulassungsinhaber immer dann problematisch, wenn die Fachaufsicht und meine Behörde zur konkreten Ausgestaltung der Videoüberwachung unterschiedliche Auffassungen vertreten. Treffe ich eine Anweisung oder eine Beschränkung gemäß Datenschutz-Grundverordnung (DS-GVO), die der Ansicht des MF widerspricht, ist diese unter Umständen nicht umsetzbar. Denn um ihre Zulassung zu behalten, sind Betreiberinnen und Betreiber verpflichtet, die Vorgaben der Fachaufsichtsbehörde umzusetzen. In der Regel konnte ich mich mit der Fachaufsicht auf eine übereinstimmende Sicht verständigen. Einzig hinsichtlich einzelner (weniger) Kameraeinstellungen war dies bisher nicht möglich.

Beschwerde eines Betriebsrates führt zu Prüfung

Hierzu ein Beispiel: Mir lag die Beschwerde eines Betriebsrates zur Videoüberwachung einer Spielbank vor, wonach auch Beschäftigte außerhalb der Spieltische in die Überwachung einbezogen würden, beispielsweise durch die Überwachung der Personaleingänge und im Rezeptionsbereich. Ich leitete daraufhin ein aufsichtsbehördliches Prüfverfahren ein. Die von mir beanstandeten Kameraeinstellungen wurden der Fachaufsicht weitergeleitet. Zunächst wurden alle erbetenen Änderungen vorgenommen. Vor Abschluss des Verfahrens bat ich darum, die Erkenntnisse aus diesem Verfahren auch in den anderen Niederlassungen umzusetzen und mir anschließend die vollständige Dokumentation zu übersenden.
Hierbei musste ich feststellen, dass die Überwachung verschiedener Bereiche erneut Anlass für Beanstandungen gab. Diese wurden wiederum dem MF zugeleitet, mit der Bitte, den von mir geforderten Änderungswünschen zu entsprechen. Dieses Mal wurden einige der genannten Punkte von der Fachaufsicht abgelehnt. Zur Begründung teilte mir das Finanzministerium mit, dass die fraglichen Erfassungsbereiche einzelner Kameras für einen effektiven Schutz der öffentlichen Sicherheit und Ordnung vor Gefahren erforderlich und von § 10 c SpielbG gedeckt seien.

In Fällen, in denen das Finanzministerium gegenüber den Spielbanken aufgrund der Videoüberwachung die Untersagung des Spielbetriebs in Aussicht gestellt hat, suche ich zur Klärung direkt den Kontakt mit dem Ministerium.

Lösung: Änderung der bestehenden Regelungen

Eine Lösung des Problems könnte durch eine Novellierung der Niedersächsischen Spielordnung (NSpielO) erreicht werden. Voraussetzung wäre, dass in der NSpielO detailliert festgelegt wird, welche Bereiche von der Videoüberwachung erfasst werden dürfen. Dabei muss allerdings sichergestellt sein, dass die festgelegten Erfassungsbereiche nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit widersprechen. So habe ich zu einem im Berichtszeitraum übersandten Referentenentwurf zur Änderung der NSpielO darauf hingewiesen, dass eine Videoüberwachung nicht für alle der dort genannten Bereiche zur Zweckerreichung notwendig ist.

Alternativ wäre es möglich, das NSpielbG so zu ändern, dass die datenschutzrechtliche Verantwortlichkeit grundsätzlich beim MF liegt. Der Betreiber oder die Betreiberin wäre dann als Auftragsverarbeiter nach Artikel 28 DS-GVO zu betrachten. Ich würde mich dann zuvorderst an das MF als Verantwortlichen wenden.

9.4 Zunehmende Beschwerden über private Videoüberwachung

Im Vergleich zum Vorjahr haben sich die Beschwerden zur Videoüberwachung durch Privatpersonen 2020 verdoppelt, auf insgesamt 171. Dabei stieg der Anteil der unbegründeten Beschwerden überproportional.

Der Einsatz von Überwachungskameras im privaten Bereich mit direktem Zugriff über mobile Endgeräte hat zugenommen. Zudem haben die Bürgerinnen und Bürger während der Corona-Pandemie mehr Zeit in ihrer häuslichen Umgebung verbracht. Diese Umstände gepaart mit einem gestiegenen Bewusstsein der Betroffenen für den mit der Videoüberwachung verbundenen Überwachungsdruck haben die Beschwerdeanzahl in meinem Haus in die Höhe schnellen lassen.

Bei der Bearbeitung der eingegangenen Beschwerden hat sich jedoch gezeigt, dass es sich dabei vermehrt um die Fortsetzung bestehender Nachbarschaftsstreitigkeiten mit anderen Mitteln handelt. Ein wachsender Anteil der Beschwerden zur privaten Videoüberwachung hat sich nach meiner Prüfung als völlig unbegründet herausgestellt.

An sich ist die Rechtslage relativ einfach: Die Befugnis zur Videoüberwachung endet grundsätzlich an der eigenen Grundstücksgrenze. Jedoch ist die eigentliche Ausrichtung der Kamera und damit der genaue Erfassungsbereich mit eventuell verpixelten/geschwärzten Bereichen oft für Außenstehende nicht erkennbar. Sie wissen so nicht, ob eine private Videoüberwachungsanlage nur das jeweilige Grundstück, sondern auch öffentlichen Raum wie Gehwege und Straßen oder das Nachbargrundstück miterfasst. Auch Attrappen sind häufig nicht auf den ersten Blick zu erkennen.

Orientierungshilfe zur Videoüberwachung durch nicht-öffentliche Stellen: https://t1p.de/OHVideoueberwachung

Statt eine (unnötige) Beschwerde wegen einer vermeintlichen Überwachung durch die Nachbarn an die Aufsichtsbehörde zu richten, wäre oft ein offenes Gespräch über die Ausrichtung der Kameras die bessere Lösung. So könnten Belastungen im Nachbarschaftsverhältnis verhindert oder zumindest gemindert werden.

J.10. Vereine/Verbände/Parteien/ Kammern

10.1 Datenverarbeitung beim Ausschluss von Vereinsmitgliedern

(Ehemalige) Vereinsmitglieder beschwerten sich bei mir über die Verarbeitung ihrer personenbezogenen Daten durch den Verein im Rahmen von Ausschlussverfahren. Dabei kritisierten sie, dass die Vereine personenbezogene Daten aus öffentlichen Quellen außerhalb des Vereins (Zeitung, Soziale Medien etc.) oder Daten, die ihnen von Dritten übermittelt wurden, zum Anlass nahmen, um Mitglieder auszuschließen. Nach Auffassung der Beschwerdeführenden war diese Datenverarbeitung durch den Verein unzulässig.

Datenverarbeitung zur Erfüllung eines Vertrags zulässig

Verarbeitet ein Verein personenbezogene Daten der Vereinsmitglieder im Rahmen eines Vereinsausschlusses kommt als rechtliche Grundlage Art. 6 Abs. 1 S. 1 lit. b der Datenschutz-Grundverordnung (DS-GVO) in Betracht. Nach dieser Vorschrift ist eine Verarbeitung nur zulässig, soweit sie für die Erfüllung eines Vertrages erforderlich ist. Unter einem solchen Vertrag ist auch die Mitgliedschaft in einem Verein zu verstehen. Zur Erfüllung eines vertraglichen Schuld- bzw. Mitgliedschaftsverhältnisses zählen auch die Beendigung und etwaige nachvertragliche Sorgfaltspflichten, denn diese ergeben sich unmittelbar aus dem Vertrags- bzw. Mitgliedschaftsverhältnis. Dies gilt auch für die Durchführung eines Ausschlussverfahrens, in dem Feststellungen über ein Mitgliedschaftsverhältnis getroffen werden sollen.

Verein darf Informationen nutzen

Im Rahmen einer vereinsinternen Untersuchung, ob eine Mitgliedschaft im Einklang mit dem Vereinszweck oder der Satzung steht bzw. ein Mitglied sich vereinsregelkonform verhält, darf ein Verein die ihm vorliegenden Informationen

in seine Bewertung einbeziehen. Es muss ihm möglich sein, sich sowohl mit öffentlich zugänglichen, anonym zugespielten als auch mit sonstigen, im Zusammenhang mit der Mitgliedschaft stehenden Informationen zu befassen und sie zur Grundlage seiner Einschätzung zu machen.

Ich leitete gegenüber den Verantwortlichen Beschwerdeverfahren ein und forderte sie zur Stellungnahme auf. Schlussendlich wurde die Verarbeitung personenbezogener Daten nach eingehender Prüfung und rechtlicher Würdigung der Stellungnahmen als gerechtfertigt angesehen. Dieses Ergebnis wurde den Beschwerdeführenden mitgeteilt, die Verfahren wurden beendet.

10.2 Kundenakquise durch Auswertung von Traueranzeigen

Ein Verein, der sich auf christlichen Beistand in schwerer Zeit spezialisiert hatte, wertete die Traueranzeigen der örtlichen Tagezeitung aus und glich diese mit dem Telefonbuch ab. An die so ermittelte Adresse wurde dann ein Brief mit Trauerrand versandt, der eine Druckschrift mit Missionierungscharakter beinhaltete sowie eine vorgedruckte Postkarte zur Anforderung von Büchern, Schriften, Bibelfernkursen und CDs.

Recht auf Auskunft nach Art. 15 DS-GVO

Eine der vom Verein angeschriebenen Personen hatte jedoch gar keinen Trauerfall und wandte sich schon deshalb sehr irritiert an mich. Ich empfahl zunächst das Auskunftsrecht aus Art. 15 Datenschutz-Grundverordnung (DS-GVO) gegenüber dem Verein geltend zu machen. Wird eine verantwortliche Stelle (sei es wie hier ein kleiner Verein, sei es ein großes Unternehmen) von einer betroffenen Person angeschrieben und um Auskunft über die dort zu dieser Person gespeicherten personenbezogenen Daten ersucht, muss sie binnen eines Monats hierüber Auskunft erteilen. Die Auskunft muss alle in Art. 15 Abs. 1 DS-GVO festgelegten Informationen und Hinweise enthalten, u.a. auch eine Angabe über die Herkunft der Daten.

Der Verein antwortete dem Betroffenen zwar binnen weniger Tage, doch entsprach dieses Schreiben nicht den Anforderungen der DS-GVO. Daraufhin wandte sich die betroffene Person erneut an mich.

Aufforderung zur Stellungnahme

Im nun eingeleiteten Kontrollverfahren forderte ich den Verein zur Stellungnahme auf. Dabei merkte ich an, dass die dem Beschwerdeführer erteilte Auskunft inhaltlich nicht den Anforderungen des Art. 15 DS-GVO genügte und ersuchte zugleich, dem Betroffenen vollumfänglich Auskunft zu erteilen. Gemäß Art. 58 Abs. 2 lit. c DS-GVO habe ich als Aufsichtsbehörde auch die Befugnis den Verein anzuweisen, dem Antrag von Betroffenen auf Ausübung des ihnen zustehenden Auskunftsrechts zu entsprechen.

Auch Informationspflichten nicht erfüllt

Der Verein übersandte mir jedoch lediglich eine Kopie der bereits vorliegenden und als unzureichend bewerteten Auskunft. Erst nach einem Auskunftsheranziehungsbescheid unter Androhung von Zwangsgeld wurde dem Beschwerdeführer Auskunft erteilt. Darüber hinaus war sich der Verein seinen Transparenz- und Informationspflichten nach Art. 13 und 14 DS-GVO nicht bewusst. Wäre dies der Fall gewesen, so hätte er bei seinem Brief an den vermeintlich Trauernden nämlich ein Informationsblatt gem. Art. 14 DS-GVO beigelegt, aus welchem sich für den Adressaten ergeben hätte, woher der Verein seine Daten hat.

Verein wird verwarnt

Das eingeleitete aufsichtsbehördliche Verfahren beendete ich mit einer Verwarnung gem. Art. 58 Abs.2 lit. b DS-GVO, da der Verein seinen Informationspflichten aus Art. 14 DS-GVO nicht nachgekommen war und mit seiner Auskunft gegenüber dem Beschwerdeführer gegen die inhaltlichen Anforderungen des Art. 15 Abs. 1 i.V.m. Art. 12 Abs. 1 DS-GVO für eine Auskunft verstoßen hatte. Der Verein hatte zudem die Kosten des Verfahrens zu tragen, da er durch sein Handeln Anlass zu dem Verfahren gegeben hatte.

10.3 Nutzung der E-Mail-Adressen von Kammermitgliedern zur Wahlwerbung

Im Berichtszeitraum erhielt ich Anfragen dazu, ob eine Berufskammer die E-Mail-Adressen ihrer Mitglieder zur Nutzung in kammerinternen Wahlkämpfen herausgeben darf. Die Antwort hierauf kann je nach Kammersatzung unterschiedlich ausfallen.

Zahlreiche Bürgerinnen und Bürger in Niedersachsen sind in Berufskammern organisiert. Die Mitgliedschaft dient der Selbstverwaltung des jeweiligen Berufsstandes und ist verpflichtend. Die Berufskammern sind Verantwortliche für die gespeicherten personenbezogenen Daten der Mitglieder. Das wichtigste Organ der Kammer ist die Kammerversammlung, quasi das „Parlament" innerhalb der Berufskammer, das über wesentliche Angelegenheiten wie z.B. den Erlass von Satzungen entscheidet. Die Kammerversammlung wird in regelmäßigen Abständen von den Mitgliedern gewählt. Die Kandidatinnen und Kandidaten für die Wahl stellen sich im Rahmen ihres Wahlkampfs den Kam-

mermitgliedern in ihrem regionalen Bezirk vor. In diesem Zusammenhang treten Kandidatinnen und Kandidaten im Vorfeld der Wahl häufig an die jeweilige Kammer heran und beantragen, dass sie ihnen die Adressen anderer Mitglieder zweckgebunden für den Zeitraum des Wahlkampfs zur Verfügung stellt. Dieselbe Interessenlage besteht bei Kandidatinnen und Kandidaten, die für die Wahl des Kammervorstands antreten.

Selbes Gesetz – zwei verschiedene Antworten

Die Anfragen, die mich hierzu erreichten, betrafen zwei niedersächsische Berufskammern. Die Gesetzeslage war identisch, für beide Kammern galt das Kammergesetz für die Heilberufe (HKG). Nach Prüfung fiel meine Antwort jedoch gegensätzlich aus – einmal war die Herausgabe zulässig, einmal nicht. Der Grund lag im Gestaltungsspielraum, der sich aus der jeweiligen Satzung der Berufskammer ergab. Die beiden Kammern hatten sich hier für einen unterschiedliche Wege entschieden.

Die Kammer hat einen Gestaltungsspielraum

Kammer A – Übermittlung zulässig

Eine Kammer hatte einem Kandidaten für dessen Wahlwerbung die E-Mail-Adressen einer Vielzahl von Mitgliedern auf Antrag übermittelt. Die Übergabe erfolgte auf sicherem Weg. In seiner E-Mail an die Wahlberechtigten informierte der Kandidat in transparenter Weise über den Hintergrund seines Schreibens. Zudem teilte er den Empfängern mit, dass er sich verpflichtet hatte, die Adressen nach Abschluss des Wahlkampfs zu löschen.

Empfänger der Wahl-Mail erhebt Beschwerde

Einer der Empfänger erhob in diesem Zusammenhang Beschwerde gegen die Kammer und wendete sich gegen die Übermittlung seiner E-Mail-Adresse an den Kandidaten. In meiner Prüfung kam ich zu folgendem Ergebnis: Trotz der Selbstverwaltung benötigt die jeweilige Kammer eine ausdrückliche gesetzliche Rechtsgrundlage. Eine bloße Satzungsregelung würde daher nicht genügen. Zudem kann nicht unmittelbar auf Rechtsgrundlagen der Datenschutz-Grundverordnung (DS-GVO) zurückgegriffen werden. Aufgrund des sogenannten Über-/Unterordnungsverhältnisses bei öffentlichen Stellen wie der Kammer verlangt die DS-GVO in Art. 6 Abs. 2, 3 DS-GVO eine fachspezifische ausdrückliche Verarbeitungsbefugnis im nationalen bzw. niedersächsischen Recht.

Kandidat hat berechtigtes Interesse glaubhaft gemacht

Das HKG enthält zwar eine Befugnis, innerhalb der Kammer personenbezogene Daten zu verarbeiten. Da aber ein Kandidat oder eine Kandidatin kein Organ der Kammer ist, kann eine Übermittlung der Daten an einen Kandidaten nicht auf § 85 a Abs. 1 HKG gestützt werden. Entscheidend war im vorliegenden Fall, dass gemäß § 85 Abs. 5 HKG das Niedersächsische Datenschutzgesetz (NDSG) unberührt bleibt. Damit ist die Übermittlungsregelung des § 5 Abs. 1 S. 2 Nr. 2 NDSG anwendbar. Nach dieser Regelung ist die Übermittlung an eine nicht-öffentliche Stelle zulässig, soweit die empfangende Stelle ein berechtigtes Interesse glaubhaft macht und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an der Geheimhaltung überwiegt. Zugleich hat sich der Empfänger bzw. die Empfängerin gegenüber der übermittelnden Stelle zu verpflichten, die Daten nur für den Zweck zu verarbeiten, zu dem sie übermittelt wurden. Diese Voraussetzungen des § 5 Abs. 1 S. 2 Nr. 2 NDSG waren erfüllt. Der Kandidat hatte durch seinen Antrag bei der Kammer ein berechtigtes Interesse an einer Verwendung der Daten glaubhaft gemacht.

Kammersatzung ist entscheidend

Entscheidend war nun, dass die Kammer in einer konkretisierenden Satzungsregelung Einzelheiten zu dieser Konstellation geregelt hatte. Insbesondere war in der Satzung vorgesehen, dass die einzelnen Kammermitglieder durch Widerspruch mitteilen können, wenn sie mit einer solchen Datenübermittlung zu Wahlwerbungszwecken nicht einverstanden sind. Im Fall eines Widerspruchs würde das schutzwürdige Interesse des Mitglieds überwiegen.

Regelmäßiger Hinweis auf Recht auf Widerspruch

Zudem sah die Kammersatzung vor, dass jedes Mitglied bei Aufnahme über diese Widerspruchsmöglichkeit informiert wird und regelmäßig im Kammermagazin nochmals darauf hingewiesen wird. Diese turnusmäßige Transparenz sprach gegen ein Überwiegen schutzwürdiger Interessen des Mitglieds. Zudem hatte das Mitglied, das sich bei mir beschwerte im Vorfeld keinen Widerspruch bei der Kammer eingelegt. Auch andere Anhaltspunkte für ein Überwiegen der Interessen des Mitglieds lagen nicht vor. Die Datenübermittlung stützte sich daher auf die Ermächtigungsgrundlage des § 5 Abs. 1 S. 2 Nr. 2 NDSG i.V.m. der genannten Satzungsregelung. Daher lag kein Datenschutzverstoß vor.

Kammer B – Übermittlung unzulässig

In dem anderen Fall handelte es sich um eine Beratungsanfrage. Hier war es umgekehrt – ein Kammermitglied begehrte die Herausgabe solcher Mitgliederadressen für den eigenen Wahlkampf. Die Kammer lehnte dies jedoch ab. Nach Prüfung kam ich zu dem Ergebnis, dass kein Anspruch des Mitglieds auf eine solche Herausgabe besteht. Zwar könnte die Kammer die selbständige Entscheidung treffen, den oben aufgezeigten Weg zu gehen, d. h., sich für eine Datenübermittlung im Wege des § 5 Abs. 1 S. 2 Nr. 2 NDSG zu entscheiden und die damit verbundene Interessenabwägung in ihrer Satzung in transparenter Weise zu konkretisieren. Die Kammer hatte sich allerdings dafür entschieden, die Interessen der Mitglieder an deren personenbezogenen Daten generell höher zu bewerten als die Interessen von Kandidatinnen und Kandidaten für eine Wahlwerbung. In dieser Konstellation fehlte es bereits an einer Satzungsregelung einschließlich Widerspruchsmöglichkeit und Transparenz, die bei der Abwägung für eine Herausgabe gesprochen hätte. Die Voraussetzungen des § 5 Abs. 1 S. 2 Nr. 2 NDSG für eine rechtmäßige Übermittlung wären ohne eine solche Satzungsregelung angesichts der hohen Quantität der Daten und der Regelmäßigkeit der Übermittlung in solchen Fällen nur schwer zu erfüllen gewesen. Es bestand daher kein Herausgabeanspruch des Kandidaten.

Kein Anspruch auf Herausgabe

Ein Recht der Kammer ist keine Pflicht

Die einzelne Kammer darf zwar mithilfe einer entsprechenden Satzungsregelung Adressen zu kammerinternen Wahlwerbezwecken herausgeben, sie muss es jedoch nicht. Sofern sich eine Kammer entscheidet, derartige Daten nicht herauszugeben, besteht kein Anspruch des Kandidaten oder der Kandidatin auf Herausgabe. Vielmehr hat es die Kammer selbst in der Hand, ob sie von der Übermittlungsbefugnis des § 5 Abs. 1 S. 2 Nr. 2 NDSG – insbesondere mithilfe einer konkretisierenden Satzung – Gebrauch machen möchte. Ein Recht auf der einen Seite führt noch nicht zu einem Herausgabeanspruch auf der anderen Seite.

10.4 Anforderungen an eine kircheneigene spezifische Aufsichtsbehörde

Eine kirchliche Glaubensgemeinschaft mit Hauptsitz in Niedersachsen teilte mir mit, dass sie meiner datenschutzrechtlichen Aufsicht entzogen sei. Die Kirche berief sich darauf, dass sie eigene umfassende Datenschutzregeln anwende und dass die datenschutzrechtliche Aufsicht durch eine von ihr eingerichtete, unabhängige Aufsichtsbehörde spezifischer Art ausgeübt werde.

Art. 91 Abs.1 Datenschutz-Grundverordnung (DS-GVO) ermöglicht es einer Kirche oder religiösen Vereinigung oder Gemeinschaft, die zum Zeitpunkt des Inkrafttretens der DS-GVO umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung angewendet hat, diese weiter anzuwenden. Voraussetzung ist, dass die Vorschriften mit der DS-GVO in Einklang gebracht wurden. Ist dies der Fall, besteht nach Art. 91 Abs. 2 DS-GVO die Berechtigung, eine eigene spezifische Aufsichtsbehörde einzurichten.

Nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) handelt es sich bei Art. 91 DS-GVO um eine Bestandsschutzregelung für Datenschutzvorschriften derjenigen Kirchen und religiösen Vereinigungen oder Gemeinschaften, die zum Zeitpunkt des Inkrafttretens der DS-GVO bereits ein umfassendes, in sich abgeschlossenes Datenschutzrecht etabliert hatten. Solche Religionsgemeinschaften sollen nicht gezwungen sein, ihr unter dem alten Recht bereits etabliertes Recht abschaffen zu müssen.

DSK-Beschluss zu spezifischen Aufsichtsbehörden: https://t1p.de/spez-aufsicht

Für Religionsgemeinschaften, die erst nach dem Inkrafttreten der DS-GVO umfassende Datenschutzvorschriften erlassen (haben), ist der sachliche Anwendungsbereich der DS-GVO uneingeschränkt eröffnet und es gilt die allgemeine Datenschutzaufsicht.

Prüfung der Datenschutzrichtlinie der Kirche

Nach Prüfung der von der Kirche eingereichten Unterlagen kam ich zu dem Ergebnis, dass die Voraussetzungen des Art. 91 DS-GVO nicht erfüllt sind. Die Datenschutzrichtlinie der Kirche enthielt jedenfalls an dem aus meiner Sicht maßgeblichen Stichtag des 25. Mai 2016 keine umfassenden Regeln zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Hierfür fehlte ein geschlossenes System mit dem Anspruch auf Vollständigkeit, welches nicht durch staatliche Regeln ergänzt werden muss. Aufgrund des gesetzlichen Stichtagsprinzips konnte ich die nach dem 25. Mai 2016 erfolgte Überarbeitung und Erweiterung der kirchlichen Datenschutzrichtlinie nicht mehr berücksichtigen. Die Tatbestandsvoraussetzungen für eine Anerkennung als spezifische Aufsichtsbehörde sind somit nicht gegeben. Daher unterliegt die Kirche meiner datenschutzrechtlichen Aufsicht.

Unterschiedliche Auffassungen über entscheidenden Stichtag

Dagegen machte die Kirche u. a. geltend, dass Art. 91 DS-GVO nicht als starre Stichtagsregelung verstanden werden dürfe, sondern von ihrem Sinn und Zweck ausgehend so zu verstehen sei, dass es nicht auf den Zeitpunkt des Inkrafttretens der DS-GVO, sondern auf deren Geltungsbeginn (25. Mai 2018) ankomme. Außerdem sei bei der Anwendung des Art. 91 DS-GVO eine Güterabwägung vorzunehmen, die im Ergebnis der Freiheit des religiösen Lebens und Wirkens den Vorzug vor staatlicher Aufsicht geben müsse. Diese Erwägungen kann ich zwar nachvollziehen, halte die geäußerte Ansicht jedoch nicht für zutreffend. Art. 91 DS-GVO bezieht sich nach seinem Wortlaut eindeutig auf den Zeitpunkt des „Inkrafttretens" der DS-GVO, nicht auf den Zeitpunkt von deren Geltungserlangung. Im Übrigen kann die Kirche ihre Angelegenheiten nur innerhalb der allgemeinen Gesetze selbst regeln, wozu auch die Regelung des Art. 91 Abs. 1 DS-GVO gehört.

Ich führte einen intensiven Dialog mit der Kirche und teilte ihr meine Rechtsauffassung mit. Die Kirche hält allerdings an ihrer Auffassung fest, dass sie die Voraussetzungen des Art. 91 DS-GVO erfülle und daher nicht meiner Aufsicht unterliege und hat eine entsprechende Feststellungsklage eingereicht. Ich begrüße es, dass nun über die strittigen Fragen eine gerichtliche Klärung herbeigeführt wird.

J.11. Technik

11.1 Datenschutzkonferenz veröffentlicht Bausteine des Standard-Datenschutzmodells

Nachdem im Jahr 2019 das Standard-Datenschutzmodell (SDM) komplett überarbeitet worden war, konnten die Arbeiten zur Erstellung, Überarbeitung und Abstimmung der Bausteine des Maßnahmenkataloges wieder aufgenommen werden. Im Jahr 2020 wurden die ersten sieben Bausteine der Datenschutzkonferenz veröffentlicht.

Mit dem Standard-Datenschutzmodell bietet die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) den Verantwortlichen in Wirtschaft und Verwaltung eine Unterstützung an, um die rechtlichen Anforderungen der Datenschutz-Grundverordnung (DS-GVO) in technisch-organisatorische Maßnahmen (TOM) zu transformieren. Sichergestellt wird dies durch den methodischen Ansatz der sogenannten Gewährleistungsziele, mit denen die rechtlichen Anforderungen strukturiert und lückenlos mit den erforderlichen TOM zusammengeführt werden. Mit der im November 2019 grundlegend überarbeiteten Version des SDM wurde die Basis für die weiteren Arbeiten geschaffen. Die 2020 verabschiedete Version 2.0b enthält gegenüber der Version 2.0 redaktionelle Änderungen und Hinweise zur Verbindlichkeit der Maßnahmen des Referenzkataloges.

Informationen zum Standard-Datenschutzmodell: https://t1p.de/SDM

Auf den Maßnahmen des Referenzkataloges lag 2020 der Schwerpunkt der Arbeiten, sodass erstmals gemeinsame Bausteine der DSK freigegeben und veröffentlicht werden konnten. Zurzeit stehen die folgenden sieben Bausteine bereit und werden zur Anwendung empfohlen:

- Baustein 11 „Aufbewahren“: Personenbezogene Daten müssen für die gesamte zulässige Verarbeitungszeit gespeichert und bereitgestellt werden.
- Baustein 42 „Dokumentieren“ umfasst die Beschreibung der Verarbeitungstätigkeit und dient dazu, die rechtmäßige Verarbeitung dauerhaft sicherstellen und nachweisen zu können.
- Baustein 43 „Protokollieren“ macht eine Verarbeitungstätigkeit, die in der Vergangenheit stattfand, prüfbar.
- Baustein 50 „Trennen“: Personenbezogene Daten dürfen nur für ihren Zweck verarbeitet werden und müssen insbesondere von „benachbarten“ Verarbeitungstätigkeiten abgegrenzt werden.
- Baustein 60 „Löschen und Vernichten“: „Löschen“ beschreibt das unkenntlich machen gespeicherter personenbezogener Daten, „Vernichten“ beschreibt hingegen die Zerstörung des Datenträgers.
- Baustein 61 „Berichtigen“: Der Verantwortliche muss gewährleisten, dass gespeicherte personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind.
- Baustein 62 „Einschränkung der Verarbeitung“ bedeutet das Markieren gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

Diese Bausteine enthalten passgenaue Maßnahmen für datenschutzkonforme Verarbeitungstätigkeiten. Mit ihnen sollen die sieben Gewährleistungsziele Datenminimierung, Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz und Intervenierbarkeit sichergestellt und eingehalten werden. Zukünftig sollen diese Bausteine durch weitere ergänzt werden.

Englische Version verfügbar

Die 2020 verabschiedete Version 2.0b ist auch in englischer Sprache verfügbar. Die DSK empfiehlt den Verantwortlichen in Wirtschaft und Verwaltung das SDM und die Bausteine anzuwenden.

7.2 Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise

Ich habe im Tätigkeitsbericht 2019 bereits meine Arbeiten zur datenschutzrechtlichen Bewertung von Windows 10 ausführlich dargestellt. Die Analysen und Auswertungen wurden im Jahr 2020 konsequent fortgesetzt.

Bei meiner Überprüfung ging es im Wesentlichen um die Frage, ob die Telemetriedatenübertragung beim Betrieb von Windows 10 vollständig mit Betriebssystemmitteln unterbunden werden kann. Unter Telemetriedaten werden Kennzahlen, Statusinformationen und Fehlermeldungen verstanden, die das Betriebssystem Windows 10 an Microsoft im Hintergrund übermittelt. Übereinstimmend betrachten sowohl die Datenschutzbehörden als auch Microsoft diese als personenbeziehbare Daten im Sinne des Datenschutzrechts. Der Umfang der Datenübermittlung wird dabei über vorkonfigurierte Stufen eingestellt, die ab Version 1903 als „Diagnosedaten aus“ (davor: Security), „Erforderlich“ (davor: Einfach) und „Optional“ (davor: Vollständig) bezeichnet werden.

Untersuchung im IT-Labor

Die Untersuchung wurde durch die Mitarbeiterinnen und Mitarbeiter meines IT-Labors vorgenommen. Die Infrastruktur des Labors gestattet es, in einer technisch geschützten und komplett vom Landesnetz abgeschotteten Umgebung Komponenten der Informations- und Kommunikationstechnik mittels Analysetools zu untersuchen. Insbesondere lassen sich im IT-Labor gezielt bestimmte, wohldefinierte Systemkonfigurationen aufbauen, ohne damit in die sonstigen Dienste des Landesnetzes einzugreifen oder diese zu stören. Schließlich lassen sich über das Labor auch Untersuchungen und Beweissicherungen im Internet vornehmen, die ansonsten an den IT-Sicherheitseinrichtungen zum Schutz der internen Datennetze scheitern würden. Ich freue mich besonders, dass mir neben diesen besonderen infrastrukturellen Gegebenheiten auch hochqualifizierte Mitarbeiterinnen und Mitarbeiter zur Verfügung stehen, um Analysen und Simulationen sachgerecht durchführen und auswerten zu können.

Unterbinden der Übertragung von Telemetriedaten ist möglich, aber aufwändig

So wurde im IT-Labor Windows 10 in der Enterprise-Edition in Version 1909 und dem Telemetrielevel „Security“ untersucht. Für diese Konfiguration gibt Microsoft an, dass unter Anwendung eines weiteren, von Microsoft bereitgestellten Patches, keine Übermittlung von Telemetriedaten stattfindet. Durch meine Untersuchung konnten die Aussagen von Microsoft nicht widerlegt werden. Es wurde auch unter Laborbedingungen keine Übertragung von Telemetriedaten festgestellt.

Position der Datenschutzkonferenz

Die Konferenz der unabhängigen Datenschutzbehörden von Bund und Ländern (DSK) fasste im November 2020 zu „Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise" einen Beschluss. Grundlagen dafür waren das datenschutzrechtlichen Prüfschema zu Windows 10, die Laborberichte meines Hauses[1], Berichte des bayerischen Datenschutzbeauftragten für den nicht-öffentlichen Bereich sowie die Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Telemetriekomponente von Windows 10 (SiSyPHus-Studie)[2]. Der Beschluss fasste die Ergebnisse verschiedener beteiligter Datenschutzaufsichtsbehörden zusammen.

Beschluss der DSK: https://t1p.de/BeschlussWindows10

Darin stellt die DSK nochmals fest, dass Verantwortliche den Nachweis für die Rechtmäßigkeit etwaiger Übermittlungen personenbezogener Daten an Microsoft zu erbringen haben oder die Übermittlung unterbinden müssen. Beim Einsatz der Enterprise-Edition können Verantwortliche die Telemetriestufe „Security" nutzen. Im Regelfall kann diese eine angemessene Maßnahme zur Unterbindung der Übermittlung von Telemetriedaten darstellen. Die bisherigen Untersuchungen können Verantwortliche nicht abschließend von der Prüf- und Nachweispflicht bei der Übermittlung von Telemetriedaten entlasten. Dies hängt mit offenen Fragen zum Aufruf der „settings-win.data.microsoft.com"-Datenverbindung zusammen (s. dazu Ausführungen im Laborbericht[3]). Zudem stellen die vorliegenden Untersuchungen aufgrund laufender Fortentwicklungen der Software nur eine Momentaufnahme dar.

Dies gilt erst recht für Verantwortliche, die Windows 10 in der Pro- oder Home-Edition einsetzen, in denen die Telemetriestufe derzeit nicht auf Security gesetzt werden kann. In diesen Fällen müssen ohnehin andere Maßnahmen zur Unterbindung etwaiger Übermittlungen personenbezogener Telemetriedaten geprüft oder die Rechtmäßigkeit der Übermittlung nachgewiesen werden.
Die DSK fordert daher, dass Windows 10 in allen angebotenen Editionen die Möglichkeit bieten sollte, die Telemetriedatenverarbeitung durch Konfiguration zu deaktivieren. Dazu und zu den in den Laboruntersuchungen in der DSK und der SiSyPHus-Studie des BSI aufgezeigten verbliebenen Unwägbarkeiten werden die Datenschutzaufsichtsbehörden weitere Gespräche mit Microsoft führen.

Stufe „Security" sollte bei allen Editionen verfügbar sein

Ausblick

Die Ergebnisse und Konfigurationsvorgaben sowie deren Bewertung durch die Datenschutzaufsichtsbehörden zur Unterbindung der Telemetrie und den Alternativen dazu sind inzwischen veröffentlicht. Ich werde daher den Einsatz von Microsoft Windows 10 im Jahr 2021 zunächst in der niedersächsischen Verwaltung prüfen, in der der Windows 10 Rollout sehr weit fortgeschritten ist.

1 https://t1p.de/konformerEinsatzWindows10
2 https://t1p.de/sisyphus
3 https://t1p.de/konformerEinsatzWindows10