Die Landesbeauftragte für den Datenschutz Niedersachsen

27. Tätigkeitsbericht 2021

27. Tätigkeitsbericht 2021

Niedersachsen

27. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für das Jahr 2021

Herausgeber: Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5, 30159 Hannover
Postfach 221, 30002 Hannover

Verantwortlich: Barbara Thiel

Layout: Thomas Kupas | design@in-fluenz.de
Lavesstraße 20/21, 30159 Hannover

Fotos: Seite 9: LfD Niedersachsen
Seite 69: Unsplash, Jonas Augustin
Seite 110: Pexels, Markus Peiske
Seite 132: Statistisches Bundesamt
alle anderen: Adobe Stock

Druck: Druckerei Albert Funke GmbH
Sorststraße 6, 30165 Hannover

Inhaltsverzeichnis

A. Vorwort

Meine Behörde und ich blicken auf ein weiteres Jahr im Zeichen der Corona-Pandemie zurück, das auch meinen Arbeitsalltag wesentlich beeinflusst hat: kaum Vor-Ort-Termine, wenig Live-Kontakt mit Kolleginnen und Kollegen und natürlich die obligatorischen Videokonferenzen. Dennoch war 2021 auch wieder ein sehr arbeits- und themenreiches Jahr, was der vorliegende Bericht verdeutlichen soll.

Zwei Entwicklungslinien, die ich schon seit Längerem beobachte, setzten sich auch im vergangenen Jahr weiter fort: Zum einen war Datenschutz nach wie vor als Thema sehr präsent, was sich unter anderem erneut an den zahlreichen Eingängen in meiner Behörde ablesen ließ. Zwar lagen die Beschwerdezahlen mit etwas mehr als 2500 nur leicht über dem Niveau des Vorjahres, dafür stiegen die von Verantwortlichen gemeldeten Datenschutzverletzungen immens an – von fast 1000 im Jahr 2020 auf mehr als 1600. Auch die Zahl der Rechtssetzungsvorhaben, in denen meine Expertise gefragt war, veranschaulicht die Bedeutung des Datenschutzes in den verschiedensten Lebensbereichen.

Besonders durch die hohe Zahl von Beschwerden und gemeldeten Datenschutzverletzungen war es mir erneut nicht möglich, in angemessenem Umfang proaktiv zu handeln. Wieder konnten beispielsweise nur wenige anlasslose Kontrollen durchgeführt werden. Auch die Art von Beratung, wie sie die Datenschutz-Grundverordnung (DS-GVO) im Sinne von Aufklärung, Sensibilisierung und Information vorsieht, kann nur punktuell erfolgen. Dies ist nicht nur misslich, sondern entspricht auch nicht der Intention der DS-GVO. Es ist absehbar, dass sich diese Situation verstetigen wird, wenn meiner Behörde nicht mehr Ressourcen zugebilligt werden.

Zum anderen musste der Datenschutz noch immer als Sündenbock für gescheiterte Vorhaben und verzögerte Prozesse herhalten. Nicht selten wurde rund um die öffentliche Diskussion zu den Corona-Maßnahmen etwa vom angeblichen „Super-Grundrecht“ gesprochen. Dabei wurde das Recht auf informationelle Selbstbestimmung (beispielsweise durch die Kontaktdatenerfassung in zahlreichen Einrichtungen) ebenso eingeschränkt wie andere Grundrechte. Das polemische, nicht immer von Fachkenntnis begleitete Narrativ vom Stolperstein Datenschutz muss endlich aufhören. Das Recht auf informationelle Selbstbestimmung ist kein Selbstzweck, sondern dient dem unmittelbaren Schutz der Privatsphäre aller Bürgerinnen und Bürger.

Barbara Thiel

Die neue Bundesregierung hat der Bedeutung dieses Rechts durch verschiedene vielversprechende Ansätze im Koalitionsvertrag Rechnung getragen. Ich hoffe, dass die neue Landesregierung nach den Wahlen im kommenden Oktober in ähnlicher Weise verfahren wird. Meine Behörde und ich werden ihr und natürlich auch der amtierenden Regierung dabei wie immer gerne beratend zur Seite stehen, sofern diese Unterstützung gewünscht wird. Sollte dies nicht der Fall sein, werde ich auch im abschließenden Jahr meiner laufenden Amtszeit nicht müde werden, regelmäßig den Finger in die Wunde zu legen und mit Nachdruck die Einhaltung der Datenschutzgesetze einzufordern. In jedem Fall ist es endlich an der Zeit, dass die Politik der Stellung und der Funktion meiner Behörde Rechnung trägt und sie so ausstattet, dass sie ihre Aufgaben in angemessener Weise erfüllen kann. Ansonsten wird es nicht möglich sein, die personenbezogenen Daten von Niedersächsinnen und Niedersachsen dauerhaft wirksam zu schützen.

B. Management Summary

Das Wichtigste in Kürze

Die europäische Zusammenarbeit der Aufsichtsbehörden nimmt weiter Fahrt auf, die Corona-Pandemie wirft zahlreiche Fragen unter anderem zur Kontaktdatenerfassung und zum Beschäftigtendatenschutz auf und Prüfungen in Landesverwaltung, Medienunternehmen sowie Krankenhäusern liefern aufschlussreiche Ergebnisse. Diese und viele weitere Themen prägten im Jahr 2021 meine Tätigkeit.

Europäische Zusammenarbeit

Der Europäische Datenschutzausschuss (EDSA) erlebte 2021 eine Premiere, als er zum ersten Mal einen verbindlichen Beschluss in einem Dringlichkeitsverfahren gemäß der Datenschutz-Grundverordnung (DS-GVO) erließ. Gegenstand des Verfahrens war ein Antrag meines Hamburger Kollegen, Maßnahmen gegen Facebook Ireland Ltd. zu verhängen, um einen Datenaustausch zwischen WhatsApp und Facebook zu verhindern. Zwar fiel die Entscheidung des EDSA nicht so aus, wie von mir erhofft. Dennoch konnte meine Behörde durch die Beteiligung am Verfahren wichtige und für die weitere Arbeit hilfreiche Erfahrungen sammeln.

Grundsatzfragen zur Bußgeldberechnung geklärt

Ebenfalls um WhatsApp ging es in einem Streitbeilegungsverfahren des EDSA. Dabei klärte der Ausschuss wichtige Grundsatzfragen, unter anderem zur Festlegung von Bußgeldern. Auch in diesem Verfahren war meine Behörde an der Ausarbeitung der EDSA-Entscheidung beteiligt.

Prüfungen zu Schrems II, Cookies und mehr

Im Bereich des internationalen Datenverkehrs begann ich 2021 gemeinsam mit weiteren deutschen Aufsichtsbehörden zu prüfen, inwieweit Unternehmen die Anforderungen aus dem Schrems-II-Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 umsetzen. Bei dieser noch nicht abgeschlossenen, anlasslosen Kontrolle steht die Einhaltung der Anforderungen für internationale Datentransfers im Rahmen des Mail- und Web-Hosting im Fokus. Es zeichnet sich ab, dass die Erfüllung der neuen Anforderungen mit großen Herausforderungen verbunden ist. In einigen Fällen erfordern sie eine grundlegende Umstellung lange praktizierter Geschäftsmodelle und -abläufe.

Eine weitere länderübergreifende Prüfung betraf die Webseiten von Medienunternehmen, die ich auf den Einsatz von Cookies und die Einbindung von Drittdiensten untersuchte. Insgesamt wurden auf Basis eines gemeinsamen Prüfkatalogs 49 Webangebote in 11 Bundesländern mit Schwerpunkt auf dem Nutzertracking zu Werbezwecken geprüft. Die meisten Webseiten entsprachen dabei nicht den rechtlichen Anforderungen für den Einsatz von Cookies und anderen Trackingtechniken. Diese Anforderungen änderten sich im Übrigen am 1. Dezember durch das Inkrafttreten des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG). Damit wurde mit zwölf Jahren Verzögerung endlich die sogenannte Cookie-Regelung der europäischen E-Privacy-Richtlinie europarechtskonform in nationales Recht umgesetzt. Als Unterstützung für alle, die das TTDSG beachten müssen, stellte ich auf meiner Webseite FAQs zur Verfügung, um grundlegende Fragen zu beantworten. Darüber hinaus positionierte sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) mit einer neuen Orientierungshilfe für Anbieter von Telemedien frühzeitig zu wesentlichen Anwendungs- und Auslegungsfragen.

Neue Anforderungen durch Inkrafttreten des TTDSG

Weitere Prüfungen im Berichtszeitraum betrafen den Einsatz von Windows 10 in Behörden der Landesverwaltung, die Videoüberwachung in Bäckereien und die Umsetzung der Datenschutz-Grundverordnung in niedersächsischen Krankenhäusern. Insgesamt machten die knappen personellen Ressourcen meiner Behörde aber nicht so viele Prüfungen möglich, wie es für eine wirksame Durchsetzung des Datenschutzrechtes nötig wäre.

Datenschutz in Zeiten der Pandemie

Natürlich wurde auch meine Tätigkeit durch die Corona-Pandemie beeinflusst. Die Datenschutzkonferenz veröffentlichte in diesem Zusammenhang mehrere Positionierungen und Orientierungshilfen, an denen ich maßgeblich beteiligt war. Im Wesentlichen ging es dabei um zwei große Themen: zum einen um die Abfrage der sogenannten 3G-Daten (geimpft, genesen, getestet) und zum anderen um die Datenerfassung zur Nachverfolgung von Kontakten. Im Zusammenhang mit Letzterem beriet ich auch das Niedersächsische Innenministerium zum Einsatz der Luca-App, auch wenn ich bedauerlicherweise in dieser Angelegenheit erst spät eingebunden wurde.

Datenschutzkonferenz beschäftigt sich mit 3G und Kontaktnachverfolgung

Auch in weiteren Zusammenhängen war meine Behörde mit den Auswirkungen der Pandemie beschäftigt. Etwa dann, wenn es um die Verwendung von Meldedaten für Impfbenachrichtigungen, um Beschwerden zu Impf- und Testzentren oder um 2G-Bändchen und die datenschutzkonforme Durchführung von Online-Prüfungen an niedersächsischen Hochschulen ging.

Mängel an der Bildungscloud bleiben

Keine erneute Prüfung der NBC geplant

Zu keinem befriedigenden Ende konnte ich leider die seit Jahren dauernde Beratung zur Niedersächsischen Bildungscloud (NBC) bringen. Das Kultusministerium übersandte mir zwar erneut eine überarbeitete Fassung des NBC-Datenschutzkonzepts, die auch eine Datenschutz-Folgenabschätzung enthielt. Wegen fortbestehender, bereits in der Vergangenheit angemerkter Änderungs- und Ergänzungsbedarfe konnte ich die NBC aus datenschutzrechtlicher Sicht wieder nicht freigeben. Schließlich musste ich dem Kultusministerium mitteilen, dass ich vor dem Hintergrund der umfangreichen, über einen langen Zeitraum und mit hohem Aufwand geleisteten Beratungen keine erneute Prüfung gegebenenfalls überarbeiteter

Unterlagen mehr durchführen kann. Zumindest werde ich aber die gewonnenen Erkenntnisse aus diesem Verfahren in die noch in der Entwicklung befindlichen „Eckpunkte für den datenschutzkonformen Einsatz von Bildungsplattformen im Schulbereich“ einfließen lassen, die den Schulen als Hilfestellung dienen sollen.

Ebenfalls als herausfordernd erwies sich einmal wieder die Zusammenarbeit mit dem Innenministerium zum Polizei-Messenger NIMes. Das Prüfverfahren zur Nutzung von NIMes auf privaten Endgeräten der Polizeibeschäftigten musste ich mit einer offiziellen Beanstandung abschließen. Das Innenministerium kündigte als Reaktion zwar die Anschaffung 5000 neuer Dienstgeräte für Polizistinnen und Polizisten an, davon wurde im Jahr 2021 aber nur ein Bruchteil ausgegeben.

Angebote zur Information und Sensibilisierung

In anderen Zusammenhängen ist die Zusammenarbeit mit der Polizei dagegen eine Erfolgsgeschichte. So konnte ich im Berichtszeitraum auf mehr als 20 Jahre Erfahrungsaustausch mit den Datenschutzbeauftragten der Polizei zurückblicken. Dieses Netzwerk erweist sich immer wieder als sehr effizient und nützlich für alle Beteiligten. Denn im Rahmen des Austausches werden datenschutzrechtliche Problemstellungen diskutiert, um bestenfalls landeseinheitliche Lösungen zu finden. Diese Pflege von Netzwerken betreibe ich auch in anderen Bereichen, zum Beispiel in Kooperation mit den Kommunen oder mit Erfahrungskreisen für Wirtschaftsunternehmen.

Konstruktiver Austausch mit den Datenschutzbeauftragten der Polizei

Überhaupt war es mir im vergangenen Jahr wieder sehr wichtig, neben meinen umfassenden Vollzugs- und Aufsichtstätigkeiten auch den Aufgaben der Beratung, Sensibilisierung und Information nachzukommen. Davon zeugen erstens meine Beteiligung an zahlreichen Rechtssetzungsvorhaben, zweitens meine Teilnahme an rund 35 Vortrags- und Diskussionsveranstaltungen und drittens die Veröffentlichung neuer Hilfestellungen zu den unterschiedlichsten Themen auf meiner Webseite. Zudem freue ich mich darüber, dass das Datenschutz-Institut Niedersachsen 2021 durch das Angebot von Online-Schulungen wieder seinen Fortbildungsbetrieb aufnehmen konnte. Dennoch bleibt festzuhalten, dass meiner Behörde auch hier die nötigen Mittel fehlen, um diesen so wichtigen Bereich der Aufklärung und Information angemessen darstellen zu können.

C. Europäischer Datenschutz

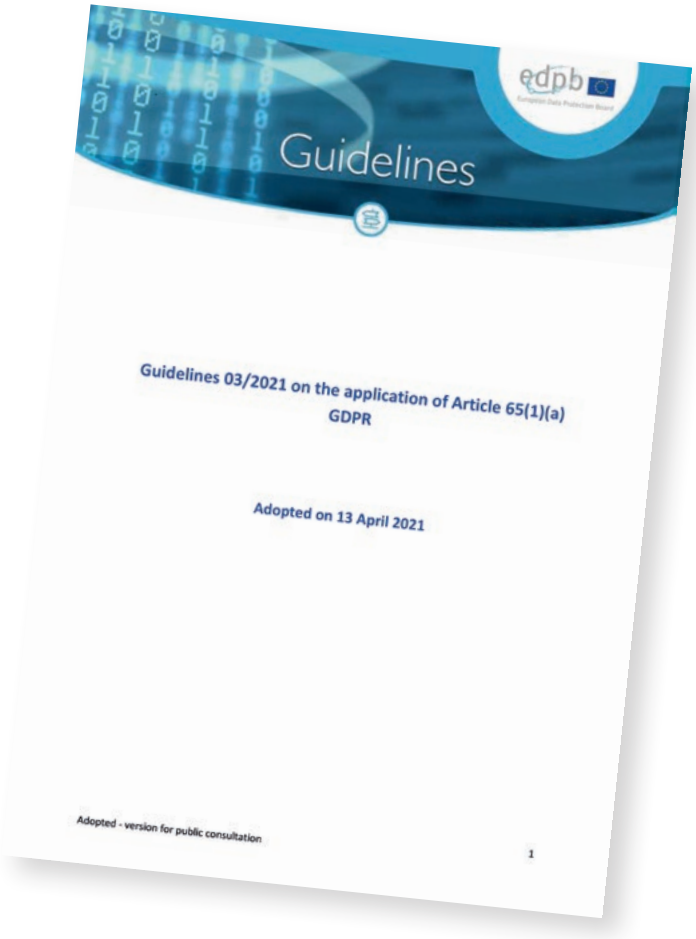
C.1. Leitlinien zum Streitbeilegungsverfahren verabschiedet

Der Europäische Datenschutzausschuss (EDSA) hat im April 2021 die Leitlinien 03/2021 zur Anwendung des Art. 65 Abs. 1 lit. a DS-GVO als Konsultationsfassung verabschiedet. Diese Leitlinien haben die Zielsetzung, die Vorschrift des Art. 65 Abs. 1 lit. a DS-GVO zu erläutern und insbesondere die Verfahrensregelungen zur Durchführung eines Streitbeilegungsverfahrens zu beschreiben. Meine Behörde hat am Entwurf der Leitlinien mitgearbeitet.

Leitlinien 03/2021 (PDF-Dokument): https://t1p.de/03-2021

Das Streitbeilegungsverfahren gem. Art. 65 Abs. 1 lit a Datenschutz-Grundverordnung (DS-GVO) kommt immer dann zur Anwendung, wenn im Kooperationsverfahren gem. Art. 60 DS-GVO zwischen der federführenden Aufsichtsbehörde und den betroffenen Aufsichtsbehörden kein Konsens gefunden wurde. Voraussetzung für die Einleitung eines solchen Streitbeilegungsverfahrens ist, dass mindestens eine betroffene Aufsichtsbehörde gegen einen Beschlussentwurf der federführenden Behörde einen maßgeblichen und begründeten Einspruch gem. Art. 60 Abs.4 DS-GVO einlegt. Schließt sich die federführende Aufsichtsbehörde dem maßgeblichen und begründeten Einspruch nicht an oder ist sie der Ansicht, dass der Einspruch nicht maßgeblich oder nicht begründet ist, muss sie das Streitbeilegungsverfahren gem. Art. 65 Abs. 1 lit. a DS-GVO einleiten.

Die Leitlinien bestätigen, dass es Ziel des Streitbeilegungsverfahrens ist, einen Beitrag zur kohärenten Anwendung der DS-GVO zu leisten. Dafür muss über die Meinungsverschiedenheiten zwischen den Aufsichtsbehörden, die Auslöser des Streitbeilegungsverfahrens waren, durch einen verbindlichen Beschluss des EDSA entschieden werden.



Ablauf des Streitbeilegungsverfahrens

Verbindlicher Beschluss innerhalb von höchstens zwei Monaten

Die Leitlinien stellen klar, dass der EDSA im ersten Schritt nach der Einleitung des Verfahrens die Vollständigkeit der von der federführenden Aufsichtsbehörde vorlegten Akte prüft. Sobald die Vollständigkeit festgestellt ist, hat der EDSA einen Monat Zeit, einen verbindlichen Beschluss mit einer Mehrheit von zwei Dritteln seiner Mitglieder anzunehmen. Diese Frist kann wegen der Komplexität der Angelegenheit um einen weiteren Monat verlängert werden.

Während dieses Zeitraumes entwirft eine Arbeitsgruppe, die aus dem Sekretariat des EDSA und weiteren Berichterstattern besteht, den verbindlichen Beschluss. Dieser erste Entwurf wird anschließend von einer Unterarbeitsgruppe des EDSA abgestimmt und weiterentwickelt. In diesem Verfahrensstadium haben alle Mitglieder des Ausschusses die Möglichkeit, ihren Standpunkt einzu-

bringen und Formulierungsvorschläge zu erarbeiten. Anschließend wird der Entwurf dem Plenum des EDSA zur Annahme vorgelegt. Sofern der Entwurf eine Mehrheit von zwei Dritteln findet, trifft die federführende Aufsichtsbehörde oder gegebenenfalls die Aufsichtsbehörde, bei welcher die Beschwerde eingereicht wurde, unverzüglich auf dieser Grundlage den endgültigen Beschluss. Sollte die Zwei-Drittel-Mehrheit nicht erreicht werden, hat der EDSA zwei Wochen Zeit den Beschluss mit der einfachen Mehrheit seiner Mitglieder anzunehmen. Bei Stimmengleichheit gibt die Stimme des Vorsitzes den Ausschlag.

Bedeutsame Praxisfragen

Die Leitlinien identifizieren die folgenden zwischen den Aufsichtsbehörden strittigen Fragestellungen als mögliche Gegenstände von Streitbeilegungsverfahren:

1. Das Vorliegen eines bestimmten Verstoßes gegen die DS-GVO,
2. das Vorliegen zusätzlicher oder alternativer Verstöße gegen die DS-GVO,
3. Lücken im Beschlussentwurf, die eine weitere Prüfung erforderlich machen,
4. unzureichende Sachverhaltsdarstellungen oder Begründungen im Beschlussentwurf,
5. verfahrenstechnische Aspekte und
6. die im Entscheidungsentwurf vorgesehene spezifische Maßnahme, insbesondere hinsichtlich der Berechnung der Bußgeldhöhe.

Außerdem stellen die Leitlinien klar, dass diejenigen, deren Interessen durch die Entscheidung im Streitbeilegungsverfahren beeinträchtigt werden könnten, das Recht auf eine Anhörung vor Abschluss des Streitbeilegungsverfahrens haben. Dieses Recht steht insbesondere dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter zu, an den sich der Beschlussentwurf richtet. Die Anhörung wird durch die nationalen Aufsichtsbehörden vor der Feststellung der Vollständigkeit der Akte gewährt.

Verpflichtung zu Nachermittlungen möglich

Weiter wird in den Leitlinien festgehalten, dass der EDSA auf einen maßgeblichen und begründeten Einspruch einer betroffenen Aufsichtsbehörde die federführende Aufsichtsbehörde verpflichten kann, Nachermittlungen vorzunehmen. Im äußersten Fall kann das dazu führen, dass die federführende Behörde einen neuen Vorgang anlegen und einen neuen Beschlussentwurf ausarbeiten muss. Auf diese Weise wird sichergestellt, dass die von den betroffenen Aufsichtsbehörden aufgeworfenen Fragen umfassend geprüft und bearbeitet werden und den Grundrechten der Betroffenen Rechnung getragen wird.

Zur Möglichkeit, gerichtlichen Rechtsschutz gegen den im Streitbeilegungsverfahren erlassenen verbindlichen Beschluss des EDSA zu suchen, stellen die Leitlinien klar, dass alle betroffenen Aufsichtsbehörden berechtigt sind, eine Nichtigkeitsklage gegen den verbindlichen Beschluss vor dem EuGH zu erheben. Ob auch für die Verarbeitung Verantwortliche, Auftragsverarbeiter oder Beschwerdeführer zur Erhebung einer Nichtigkeitsklage vor dem EuGH berechtigt sind, hänge davon ab, ob diese direkt und individuell betroffen seien. Ob das der Fall sei, müsse in jedem Einzelfall geprüft werden.

C.2. Erster verbindlicher Beschluss des EDSA im Dringlichkeitsverfahren

Im Jahr 2021 erließ der Europäische Datenschutzausschuss (EDSA) seinen ersten verbindlichen Beschluss in einem Dringlichkeitsverfahren gem. Art. 66 Abs. 2 Datenschutz-Grundverordnung (DS-GVO). Gegenstand des Dringlichkeitsverfahrens war ein Antrag des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI), endgültige Maßnahmen nach Art. 66 Abs. 2 DS-GVO gegen Facebook Ireland Ltd. zu verhängen, um einen Datenaustausch zwischen WhatsApp und Facebook zu verhindern. Meine Behörde war im Rahmen einer Unterarbeitsgruppe an der Ausarbeitung der EDSA-Entscheidung beteiligt.

WhatsApp hatte alle Nutzerinnen und Nutzer aufgefordert, bis zum 15. Mai 2021 neuen Nutzungs- und Privatsphäre-Bestimmungen zuzustimmen. Darin waren aus aufsichtsbehördlicher Sicht sehr weitgehende Befugnisse zugunsten von WhatsApp für Datenübermittlungen an Facebook enthalten. Insbesondere sollte es ermöglicht werden, dass Facebook die personenbezogenen Daten der WhatsApp-Nutzerinnen und -Nutzer für eigene Zwecke verarbeitet.

Der HmbBfDI hielt eine solche Datenverarbeitung durch Facebook zu eigenen Zwecken für rechtswidrig. Er hatte daher der Facebook Ireland Ltd. per einstweiliger Maßnahme nach Art. 66 Abs. 1 DS-GVO für drei Monate untersagt, personenbezogene Daten von WhatsApp-Nutzern mit Wohnsitz in Deutschland, die von WhatsApp an Facebook übertragen werden, zu eigenen Zwecken zu verarbeiten.

Der HmbBfDI war der Auffassung, dass nach dem Ablauf der drei Monate dringend endgültige Maßnahmen erlassen werden mussten. Deshalb beantragte er beim EDSA, einen Datenaustausch zwischen WhatsApp und Facebook durch den Erlass einer endgültigen Maßnahme für alle Mitgliedstaaten zu verhindern.

Der Ausgang des Dringlichkeitsverfahrens

Der EDSA lehnte den Erlass eines verbindlichen Beschlusses ab, denn er verneinte mit knapper Mehrheit das Vorliegen von Dringlichkeit. Er war der Ansicht, dass zum damaligen Zeitpunkt nicht genügend Informationen vorlagen, aufgrund derer mit Sicherheit darauf geschlossen werden könnte, dass

Facebook Ireland bereits damit begonnen hätte oder bald damit beginnen würde, die Daten von WhatsApp-Nutzenden als Verantwortlicher zu verarbeiten. Außerdem sah sich der Ausschuss nicht in der Lage anhand der vorliegenden Informationen festzustellen, dass eine Rechtsverletzung stattfindet.

Allerdings stellte der EDSA weitreichende Widersprüche fest zwischen der Ankündigung an die WhatsApp-Nutzerinnen und -Nutzer über die Verwendung ihrer personenbezogenen Daten für die Zwecke von Facebook und Zusagen Facebooks, solche Datenverarbeitungen fänden (noch) nicht statt. Daher hielt der EDSA die federführende irische Datenschutzaufsichtsbehörde (DPC) dazu an, eine weitergehende Prüfung vorzunehmen. Gegenstand der Prüfung sollen die tatsächlichen Verarbeitungsprozesse bei Facebook in Bezug auf WhatsApp-Daten und die Frage der möglichen Rechtsgrundlage dafür sein. Das Ergebnis dieser Prüfung lag zum Redaktionsschluss dieses Berichts noch nicht vor.

Bewertung der Entscheidung des EDSA

Dringende verbindliche Entscheidung 01/2021 des EDSA: https://t1p.de/01-2021

Ich hätte mir eine deutlichere Entscheidung des EDSA erhofft und habe mich auch in der Unterarbeitsgruppe, die den Entscheidungsentwurf erstellt hat, entsprechend positioniert. Die WhatsApp-Nutzerinnen und -Nutzer waren durch das Unternehmen in den aktualisierten Nutzungsbedingungen darüber informiert worden, dass Facebook ihre personenbezogenen Daten für eigene Zwecke verarbeitet. Daraus lässt sich durchaus dringender Handlungsbedarf ableiten, um die Rechte und die Freiheiten der betroffenen Personen zu schützen. Die sehr enge Auslegung des Tatbestandsmerkmals der Dringlichkeit, die im EDSA eine knappe Mehrheit fand, birgt das Risiko, dass in zukünftigen Fällen möglicherweise kein zeitnaher effektiver Schutz der Rechte und Freiheiten der Betroffenen gewährleistet werden kann.

C.3. Streitbeilegungsverfahren zu WhatsApp Ireland klärt Grundsatzfragen

Im Sommer 2021 führte der Europäische Datenschutzausschuss (EDSA) ein wichtiges Streitbeilegungsverfahren zu WhatsApp Ireland durch. Streitbeilegungsverfahren vor dem EDSA sind notwendig, wenn sich bei grenzüberschreitenden Verarbeitungen die beteiligten Datenschutzaufsichtsbehörden im Kooperationsverfahren nicht auf ein Ergebnis einer Untersuchung einigen können. Meine Behörde war an der Ausarbeitung der EDSA-Entscheidung beteiligt.

Einspruch gegen Beschluss aus Irland

Die irische Datenschutzaufsichtsbehörde (DPC) gelangte nach einer umfangreichen Untersuchung zu dem Ergebnis, dass WhatsApp Ireland bei der Zusammenarbeit mit den Facebook-Unternehmen gegen Transparenz- und Informationsverpflichtungen nach Artikel 12, 13 DS-GVO verstoßen habe. Als Abhilfemaßnahmen sollten eine Verwarnung und eine Anweisung ausgesprochen sowie eine Geldbuße verhängt werden. Verschiedene europäische Aufsichtsbehörden legten gegen diesen Beschlussentwurf Einsprüche ein. Ich habe mich an der Formulierung eines koordinierten deutschen Einspruchs be-

teiligt. Der Einspruch wurde insbesondere damit begründet, dass die im Beschlussentwurf vorgesehene Geldbuße zu gering und die Rechtsgrundlage für eine Datenweitergabe von WhatsApp an Facebook nicht geprüft worden sei.

Die Entscheidung des EDSA

Der EDSA gelangte nach mehreren Sitzungen seiner Enforcement Subgroup, in der meine Behörde die Interessen der deutschen Länder vertritt, zu dem Ergebnis, dass die DPC ihren Beschlussentwurf ändern muss. Was die Erfüllung der Transparenzpflichten betrifft, stellte der EDSA im Vergleich zur irischen Aufsicht zusätzliche Mängel fest. Die DPC wurde verpflichtet, einen Verstoß gegen Art. 13 Abs. 1 lit. d DS-GVO festzustellen. Zur Übermittlung von Telefonnummern von Nicht-Nutzern aus dem Adressbuch eines WhatsApp-Nutzers wurde festgestellt, dass das bisher von WhatsApp durchgeführte Verfahren keine Anonymisierung der personenbezogenen Daten von Nicht-Nutzern leistet. Folglich ist geklärt, dass es sich auch bei den gekürzten Hash-Werten von Telefonnummern der Nicht-Nutzer um personenbezogene Daten handelt, welche nur nach Maßgabe der DS-GVO verarbeitet werden dürfen.
Zur Berechnung von Geldbußen entschied der EDSA die sehr wichtige Grundsatzfrage, dass der Umsatz eines Unternehmens zu berücksichtigen ist, um sicherzustellen, dass die Geldbuße wirksam, verhältnismäßig und abschreckend im Sinne von Artikel 83 Absatz 1 DSGVO ist. In dem Zuge verpflichtete der Ausschuss die DPC dazu, die Höhe der Geldbuße neu zu berechnen und einen höheren Betrag festzulegen. Die DPC ist dieser Verpflichtung nachgekommen und hat die Höhe der Geldbuße auf 225 Millionen Euro festgesetzt, nachdem zuvor zwischen 30 und 50 Millionen Euro vorgesehen waren.

Bewertung der Entscheidung des EDSA

Entscheidung 01/2021 des EDSA: https://t1p.de/EDSA-DPC

Ich begrüße die Feststellungen des EDSA, dass das bisher von WhatsApp durchgeführte Verfahren bei der Erhebung von Daten von Nicht-Nutzern keine Anonymisierung der personenbezogenen Daten leistet und dass die Höhe des Umsatzes eines Unternehmens bei der Berechnung der Geldbuße zu berücksichtigen ist. Das wird in zukünftigen Verfahren dazu beitragen, den Schutz der personenbezogenen Daten der Bürgerinnen und Bürger spürbar zu verbessern. Ebenso begrüße ich, dass der EDSA die DPC zur Festlegung einer höheren Geldbuße verpflichtet hat.

Darüber hinaus hätte ich mir eine Klärung der Frage gewünscht, ob die nicht erfolgte Anonymisierung der von Nicht-Nutzern erhobenen personenbezogenen Daten zu einer Verletzung von Art. 6 DS-GVO führt. Ich hoffe, dass sich möglichst bald in einem weiteren Verfahren die Gelegenheit bietet, diese wichtige Grundsatzfrage zu klären, die Millionen von EU-Bürgerinnen und -Bürgern betrifft.

C.4. Die Arbeit der Enforcement Subgroup

Auch im Jahr 2021 hat meine Behörde die Ländervertretung in der Enforcement Subgroup des Europäischen Datenschutzes übernommen. Der Arbeitsumfang hat weiter zugenommen, was vor allem auf die Streitbeilegungs- und Dringlichkeitsverfahren zurückzuführen ist.

Die Enforcement Subgroup ist eine Fachuntergruppe des Europäischen Datenschutzausschusses (EDSA). Darin sind alle Mitgliedstaaten der Europäischen Union, Norwegen, Island und Liechtenstein als EWR-Mitgliedstaaten, der Europäische Datenschutzbeauftragte sowie die Europäische Kommission vertreten. Letztere hat jedoch kein Stimmrecht. Die Arbeitsgruppe hat die Aufgabe, die kohärente Anwendung der Abhilfebefugnisse der Datenschutz-Grundverordnung (DS-GVO) zu fördern und dadurch die Durchsetzung der Verordnung in der Praxis zu verbessern. Dies geschieht unter anderem durch den regelmäßigen Austausch zu aktuellen Fällen und durch die Entwicklung von Leitlinien. 2021 haben 14 Sitzungen der Arbeitsgruppe per Videokonferenz stattgefunden. Präsenzsitzungen in Brüssel waren wegen der Corona-Situation nicht möglich.

Durchsetzung der DS-GVO in der Praxis verbessern

Aus § 17 des Bundesdatenschutzgesetzes folgt, dass Deutschland im EDSA und seinen Fachuntergruppen nicht nur durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), sondern auch durch einen Vertreter der Länder repräsentiert wird. So haben die Länder die Möglichkeit, unmittelbar auf europäischer Ebene ihre Positionen und Interessen einzubringen. In der Enforcement Subgroup vertritt Niedersachsen die Interessen der deutschen Länder.

In der Praxis erfordert die Arbeit als Ländervertretung, dass vor jeder Sitzung bei Bedarf eine Abstimmung mit den anderen Ländern über die Positionierung zu den Themen auf der Agenda erfolgt. Sobald eine einheitliche Positionierung erreicht werden konnte, wird diese in einem zweiten Schritt mit dem BfDI abgestimmt, um ein einheitliches deutsches Auftreten in der Sitzung sicherstellen zu können. In der Arbeitsgruppe herrscht ein sehr produktives und lösungsorientiertes Arbeitsklima.

Einheitliches Auftreten der deutschen Aufsicht sicherstellen

Schwerpunkte der Enforcement Subgroup

Die Schwerpunkte der Arbeitsgruppe waren im vergangenen Jahr das Streitbeilegungsverfahren zu WhatsApp (siehe C.3, S. 19) sowie das Dringlichkeitsverfahrens in Sachen Facebook (siehe C.2, S. 17). Zudem verabschiedete die Arbeitsgruppe die Leitlinien 03/2021 zur Anwendung des Art. 65 Abs. 1 lit. a DS-GVO in der Konsultationsfassung (siehe C.1, S. 14).

Darüber hinaus wurde mit der Vorbereitung der Coordinated Enforcement Action 2022 begonnen. Die Schaffung eines verfahrenstechnischen Rahmens soll es den Aufsichtsbehörden ermöglichen, auf freiwilliger Basis jährlich eine koordinierte Vollzugsmaßnahme zu einem vorher festgelegten Thema zu ergreifen. 2022 lautet das gemeinsame Thema: „The use of cloud based services by the public sector".

Vorbereitung einer Stellungnahme des EDSA

Zum Ende des Jahres bereitete die Subgroup eine Stellungnahme des EDSA gem. Art. 64 Abs. 2 DS-GVO zu der Grundsatzfrage vor, ob Art. 58 Abs. 2 lit. g DSGVO als Rechtsgrundlage für eine Aufsichtsbehörde dienen könnte, um die Löschung personenbezogener Daten von Amts wegen anzuordnen, wenn ein solcher Antrag nicht von der betroffenen Person gestellt wurde. Die Auslegungsfrage ergab sich aus der täglichen Arbeitspraxis der Aufsichtsbehörden, da bislang unklar war, wie in einem solchen Fall zu verfahren sei.

In mehreren Sitzungen wurde ein Entwurf erarbeitet, und die Arbeitsgruppe hat sich darauf verständigt, dass Art. 58 Abs. 2 lit. g DSGVO eine taugliche Rechtsgrundlage ist. Das Plenum des EDSA ist dieser Empfehlung gefolgt und hat am 14. Dezember 2021 die entsprechende Stellungnahme 39/2021 verabschiedet. Diese hat große Bedeutung für die Arbeit meiner Behörde, weil hiermit eine für die aufsichtsbehördliche Praxis wichtige Auslegungsfrage beantwortet wurde.

C.5. Europäische Zusammenarbeit bei technischen Untersuchungen

Zusammen mit weiteren deutschen Aufsichtsbehörden sowie denen mehrerer EU-Mitgliedsstaaten und dem Europäischen Datenschutzbeauftragten (EDSB/EDPS) beteilige ich mich an der Expertengruppe „Mobile Audit Exchange", die ein europaweit abgestimmtes Vorgehen für technische Untersuchungen erarbeitet. Vom europäischen Datenschutzausschuss (EDSA) hat diese Expertengruppe im September 2021 ein entsprechendes Mandat erhalten.

Die Datenschutz-Grundverordnung (DS-GVO) gibt für alle europäischen Länder denselben rechtlichen Rahmen vor, der in einigen Bereichen durch nationale Ausgestaltungen spezifiziert werden kann. Zusätzlich bilden in Deutschland bundeslandspezifische Datenschutzregelungen den Bedarf an individuellen Regelungen der Bundesländer für den öffentlichen Bereich ab. Daher kann die juristische Bewertung von datenschutzrechtlichen Sachverhalten in verschiedenen Ländern bzw. Bundesländern, zu unterschiedlichen Ergebnissen führen.

Keine spezifischen Abweichungen bei technischer Ausgestaltung

Im Gegensatz dazu gibt es bei der eingesetzten und zu bewertenden Technik keine länderspezifisch abweichende Ausgestaltung. So ist z. B. die eingesetzte Technik bei einem Messenger, einer Smartphone-App, einem Webshop, einem SAP-System oder einer Website unabhängig davon, in welchem Land der Verantwortliche sein Verfahren betreibt. Auch die Anpassung der Benutzeroberfläche an die jeweilige Landessprache hat in aller Regel keinen Einfluss auf die Funktionalität der eingesetzten Technik. Gleichzeitig gewinnen die Analyse und Bewertung von technischen Sachverhalten durch die Digitalisierung praktisch aller Lebensbereiche immer mehr an Bedeutung.

IT-Labor für unterschiedliche Prüfsituationen

Aus diesem Grund habe ich bereits 2016 mein IT-Labor konzipiert und nach und nach für die unterschiedlichsten Prüfsituationen in Betrieb genommen. Meine Mitarbeiter haben mittlerweile vielfältige Erfahrungen gesammelt und Know-how aufgebaut. Ich bin aber der Meinung, dass nicht jede Aufsichtsbehörde selbst von Grund auf alle Entwicklungsschritte parallel zu anderen machen muss. Mein Ziel ist es, Synergien zu schaffen, indem mit anderen Aufsichtsbehörden gemeinsame Standards bei technischen Untersuchungen

festlegt werden. Auf der europäischen Ebene wird diese Zusammenarbeit in der Expertengruppe „Mobile Audit Exchange“ abgestimmt.

Konzentration auf Analyse mobiler Apps

Da nicht alle technischen Themen durch die Expertengruppe gleichzeitig bearbeitet werden können, konzentriert sich die Arbeit aktuell auf die Analyse und Bewertung von mobilen Apps. Dabei sollen für die beiden im Markt dominierenden Betriebssysteme Android und Apple-OS Prüfumgebungen und standardisierte Prüfungsabläufe festgelegt werden.

Niedersächsische und EU-Testumgebung im Vergleich

In meinem IT-Labor wurde dazu neben der von mir selbst entwickelten Testumgebung auch die bei der EU eingesetzten Umgebung zum Vergleich aufgebaut. So konnte ich weitere Erfahrungen sammeln und Vor- und Nachteile der unterschiedlichen Konzepte erkennen. Im nächsten Jahr werde ich auf Basis der gewonnenen Erkenntnisse eine optimierte Prüfumgebung realisieren und damit noch besser in der Lage sein, die juristischen Fachleute mit qualitativ hochwertigen technischen Analyseergebnissen zu unterstützen.

Neben der Standardisierung von Prüfumgebungen und Prüfabläufen im IT-Labor tauscht sich die Expertengruppe auch mit Expertinnen und Experten aus Forschung, Wirtschaft und anderen Behörden aus. Bereits 2021 wurden erste Forschungsergebnisse im Bereich Datenübermittlung von Smartphone-Betriebssystemen (Trinity College Dublin, Ireland), kommerzielle Analysen von Apps (AppCensus, Inc., Spanien) sowie Untersuchungsergebnisse des Bundeskartellamtes zu mobilen Apps von den eingeladenen Fachleuten präsentiert und fachlich diskutiert. Dieser Austausch wird im nächsten Jahr fortgesetzt. Zudem plane ich auch für das nächste Jahr die kontinuierliche Weiterqualifikation meiner technischen Mitarbeiterinnen und Mitarbeiter.

D. Internationaler Datenverkehr

D.1. Prüfung zur Umsetzung des Schrems II-Urteils durch niedersächsische Unternehmen

2021 begann ich zu prüfen, inwieweit niedersächsische Unternehmen die Anforderungen aus dem Schrems-II-Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (Rs. C-311/18) umsetzen. Bei dieser anlasslosen Kontrolle steht die Einhaltung der Anforderungen für internationale Datentransfers beim Mail- und Web-Hosting im Fokus. Die Prüfung werde ich 2022 abschließen.

Die Kontrolle von Datenübermittlungen in Länder außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (sogenannte Drittstaaten) wird von mehreren deutschen Datenschutzaufsichtsbehörden gemeinsam durchgeführt. Ziel dieser Prüfung ist die breite Durchsetzung der Anforderungen des Europäischen Gerichtshofs aus seiner Schrems-II-Entscheidung (siehe hierzu ausführlich Tätigkeitsbericht 2020, S. 27). Darin hatte das Gericht festgestellt, dass Übermittlungen personenbezogener Daten in die USA nicht länger auf Basis des sogenannten Privacy Shield erfolgen können.

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

Der Einsatz der Standardvertragsklauseln für Datenübermittlungen in Drittstaaten ist nur noch unter Verwendung zusätzlicher wirksamer Maßnahmen ausreichend, wenn die erforderliche Prüfung des Verantwortlichen ergeben hat, dass im Empfängerstaat kein gleichwertiges Schutzniveau für die personenbezogenen Daten gewährleistet werden kann. Diese Vorgaben erfordern in vielen Fällen eine grundlegende Umstellung lange praktizierter Geschäftsmodelle und -abläufe.

Erste Auswertung vermittelt positiven Eindruck

Gemeinsam mit den Landesdatenschutzbehörden aus Baden-Württemberg, Bayern, Berlin, Bremen, Brandenburg, Hamburg, Rheinland-Pfalz und dem

Saarland hat meine Behörde Fragenkataloge zum internationalen Datenverkehr erarbeitet. Auf dieser Grundlage habe ich 18 niedersächsische Unternehmen verschiedener Branchen angeschrieben und um Auskunft zu ihren datenschutzrechtlichen Vorkehrungen beim Mail- und Web-Hosting gebeten.

Link zu den Fragebögen: https://t1p.de/Fragebogen-internationaler-Datenverkehr

Eine erste Auswertung der von den Unternehmen zurückgesandten Fragekataloge hat ergeben, dass den Unternehmen erfreulicherweise grundsätzlich bekannt ist, dass sich bei der Übermittlung personenbezogener Daten in Drittstaaten besondere Anforderungen ergeben. Allerdings zeichnet sich auch ab, dass in der Praxis speziell die Erfüllung der neuen Anforderungen aus dem Schrems II-Urteil mit großen Herausforderungen verbunden ist. Bereits der Einsatz von im Unternehmensalltag etablierten Standardlösungen zum E-Mail-Versand kann unter Umständen dazu führen, dass die Anforderungen nicht vollständig erfüllt werden können. Daher kann in manchen Fällen ein Wechsel zu anderen Dienstleistern oder der Einsatz anderer technischer Lösungen für die Unternehmen erforderlich werden.

Ich beabsichtige, die Prüfung 2022 abzuschließen. Bei identifizierten Defiziten werde ich zunächst versuchen, im Dialog mit den Unternehmen die Rechtmäßigkeit der Datenübermittlungen herzustellen. Wo dies nicht möglich ist, werde ich mit aufsichtsbehördlichen Maßnahmen reagieren. Über diese Prüfung hinaus erwarte ich von allen Verantwortlichen in Niedersachsen, dass sie sich mit den neuen Anforderungen des „Schrems II"-Urteils auseinandersetzen und eigenständig nach Lösungen suchen. Ich werde mir daher vorbehalten, zukünftig auch weitere Verantwortliche in Niedersachsen entsprechend zu befragen sowie andere Themenbereiche im internationalen Datenverkehr in den Blick zu nehmen.

D.2. Neue Standardvertragsklauseln für den internationalen Datentransfer

Die EU-Kommission hat im Juni 2021 neue Standardvertragsklauseln für den internationalen Datentransfer vorgelegt. Die neuen Klauseln bilden die Anforderungen der „Schrems II"-Rechtsprechung des Europäischen Gerichtshofs (EuGH) ab und ermöglichen erstmals datenschutzrechtliche Dienstleisterketten. Verantwortliche Stellen in Niedersachsen sind bereits seit Herbst vergangenen Jahres verpflichtet, für Neuverträge die neuen Klauseln einzusetzen und müssen bis Ende 2022 sämtliche Altverträge umstellen.

Schutzniveau außerhalb des EWR erhalten

Der internationale Datenverkehr hat aufgrund der weltweiten Vernetzung enorm an Bedeutung gewonnen, zugleich sind hierdurch neue Herausforderungen für den Schutz personenbezogener Daten entstanden. Die DS-GVO will internationale Datentransfers nicht unterbinden, verfolgt aber das Ziel, dass das durch die DS-GVO unionsweit gewährleistete Schutzniveau für natürliche Personen bei der Übermittlung an Empfänger in Drittländer gewährleistet wird. Denn sind personenbezogene Daten erst einmal an Drittstaaten ohne vergleichbares Datenschutzniveau übermittelt, lassen sich diese nicht mehr immer ohne Weiteres zurückholen oder löschen. Daher ist es von grundlegender Bedeutung, dass das Schutzniveau der DS-GVO auch erhalten bleibt, wenn die personenbezogenen Daten den Europäischen Wirtschaftsraum verlassen.

Beschluss der EU-Kommission: https://t1p.de/svk

Um dies zu erreichen werden in der Praxis vor allem Standardvertragsklauseln eingesetzt. Hierbei handelt es sich um von der Europäischen Kommission verabschiedete Vertragsmuster, auf deren Grundlage europäische Datenschutzstandards vertraglich zwischen Datenexporteuren im Europäischen Wirtschaftsraum und Datenimporteuren in Drittstaaten vereinbart werden. Bei ihrer Verwendung kann die Übermittlung personenbezogener Daten in Drittländer ohne weitere Genehmigung der Aufsichtsbehörden erfolgen (Art. 46 Abs. 2 Buchstabe c DS-GVO).

Neuer modularer Aufbau

Die Europäische Kommission hat im Juni 2021 neue Standardvertragsklauseln erlassen. Vorausgegangen war ein Entwurf vom November 2020, zu welchem der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte Anfang 2021 eine gemeinsame Stellungnahme abgegeben hatten, an deren Ausarbeitung meine Behörde beteiligt war.

Stellungnahme von EDSA und EDSB: https://t1p.de/stellung-svk

Die neuen Standardvertragsklauseln sind modular aufgebaut und können in folgenden Übermittlungskonstellationen eingesetzt werden:

- Modul 1: Verantwortlicher an Verantwortlichen
- Modul 2: Verantwortlicher an Auftragsverarbeiter
- Modul 3: Auftragsverarbeiter an (Unter-)Auftragsverarbeiter
- Modul 4: Rückübermittlung durch den Auftragsverarbeiter in der EU an einen Verantwortlichen im Drittland

Während bei den alten Standardvertragsklauseln der Datenexporteur stets der Verantwortliche war, können mit dem Modul 3 nun erstmals unmittelbar Dienstleisterketten abgebildet werden, in denen der Auftragsverarbeiter personenbezogene Daten an einen Unterauftragsverarbeiter exportiert. Neu ist zudem das Modul 4, welches die Rückübermittlung von einem Auftragsverarbeiter in der Union an einen Verantwortlichen in einem Drittland abdeckt.

Mit den neuen Standardvertragsklauseln ist die Notwendigkeit entfallen, bei der Übermittlung an einen Auftragsverarbeiter zusätzlich einen Vertrag nach Art. 28 DS-GVO abzuschließen. Die Anforderungen des Art. 28 Abs. 3 und 4 DS-GVO wurden in die neuen Klauseln eingearbeitet.

„Schrems II" eingearbeitet, aber nicht gelöst

Mit dem „Schrems II"-Urteil vom 16. Juli 2020 hat der EuGH die Anforderungen an die Verwendung von Standardvertragsklauseln in der Praxis ganz erheblich verschärft (siehe dazu ausführlich meinen Tätigkeitsbericht 2020, S. 27). Danach liegt es in der Verantwortung eines Datenexporteurs, vor der Übermittlung personenbezogener Daten zu prüfen, ob in dem Drittland ein Schutzniveau für personenbezogene Daten besteht, das dem in der EU gleichwertig ist.

Dabei geht es vor allem um die Frage, ob die Vertragsparteien beim Abschluss von Standardvertragsklauseln und unter Berücksichtigung zusätzlicher Maßnahmen Grund zu der Annahme haben, dass die Rechtsvorschriften und Gepflogenheiten im Drittland den Datenimporteur an der Erfüllung seiner Pflichten aus den Standardvertragsklauseln hindern. Sofern das der Fall ist, müssen gegebenenfalls zusätzliche Maßnahmen zur Sicherstellung eines dem in der EU im Wesentlichen gleichwertigen Schutzniveaus ergriffen oder von der Übermittlung abgesehen werden.

Datenexporteur muss Rechtslage im Drittland prüfen

An dieser Situation und den sich daraus ergebenden Verpflichtungen hat sich durch die neuen Standardvertragsklauseln nichts geändert. Diese regeln lediglich die bisher aus der Rechtsprechung des EuGH folgenden Anforderungen. Der Datenexporteur muss auch bei Verwendung der neuen Klauseln die Rechtslage und -praxis des Drittlands prüfen und ggf. zusätzliche Schutzmaßnahmen ergreifen oder von der Übermittlung Abstand nehmen.

Umsetzungsfristen beachten

Verantwortliche müssen die von der Kommission gesetzten Umsetzungsfristen beachten. Bereits seit dem 27. September 2021 sind die neuen Standardvertragsklauseln zwingend für den Abschluss von Neuverträgen zu verwenden. Spätestens zum Ablauf des 27. Dezembers 2022 muss eine Umstellung sämtlicher Altverträge auf die neuen Standardvertragsklauseln erfolgt sein.

E. Datenschutzkonfenrenz

E.1. Datenschutz in der Corona-Pandemie: Aktivitäten der Datenschutzkonferenz

Während der 2021 andauernden Corona-Pandemie war die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) mit zwei großen Themen beschäftigt: Zum einen mit der Datenerfassung zur Kontaktnachverfolgung, zum anderen mit der Abfrage der sogenannten „3G-Daten" (geimpft, genesen, getestet).

CWA und Luca im Fokus der Aufmerksamkeit

Zur Erfassung der Kontaktdaten veröffentlichte die DSK fünf Papiere, welche die Kontaktnachverfolgung mit digitalen Diensten betreffen. Im Fokus der Aufmerksamkeit stand neben der Corona-Warn-App (CWA) des Robert-Koch-Instituts vor allem das System „Luca" der Berliner culture4life GmbH.

Abgesehen von den personenbezogenen Daten für die Kontaktnachverfolgung fragten Verantwortliche zudem 3G-Daten ab. Einen Schwerpunkt in der datenschutzrechtlichen Beratung und Prüfung bildeten Abfragen der 3G-Daten von Beschäftigten durch Arbeitgeberinnen und Arbeitgeber. Zu diesem Thema veröffentlichte die DSK drei Papiere.

Digitale Kontaktnachverfolgung

Ein Eckpfeiler in der Pandemie-Bekämpfung ist die schnellstmögliche und umfassende Information von Kontaktpersonen einer infizierten Person, um Infektionsketten zu unterbrechen. Grundsätzlich obliegt die Aufgabe der Kontaktnachverfolgung dem Gesundheitsamt, da dieses befugt ist, gegenüber infektionsrelevanten Kontakten einer infizierten Person Quarantäne-Anordnungen auszusprechen. Mit zeitweise schnell und stark ansteigenden Inzidenzwerten zeigte sich allerdings, dass die Gesundheitsämter bei der Kontaktnachverfolgung Unterstützung benötigen. Daher wurden 2021 zwei unterschiedliche Strategien verfolgt.

Zwei Strategien zur Nachverfolgung der Kontakte

- Erstens die Kontaktdatenerfassung und im Positivfall die anschließende Information der relevanten Kontakte durch die Bürgerinnen und Bürger

selbst. Dafür wurde die Corona-Warn-App des RKI in enger Zusammenarbeit den deutschen Aufsichtsbehörden entwickelt.
- Zweitens wurde im Infektionsschutzgesetz die Anordnung der Verarbeitung der Kontaktdaten von Kundinnen und Kunden, Gästen oder Veranstaltungsteilnehmenden als notwendige Schutzmaßnahme geregelt. Die konkrete Ausgestaltung der Pflicht zur Kontaktdatenerfassung erfolgte in den Corona-Verordnungen der Länder.

Zunächst wurden die Kontaktdaten überwiegend in Papierform erfasst. Für die Gesundheitsämter ergab sich ein eher geringer Mehrwert. Es mussten weiterhin zunächst infizierte Personen kontaktiert und anschließend bei den relevanten Betrieben und Veranstaltern die Kontaktnachweise einzeln abgefragt werden. Zudem besteht eine hohe Wahrscheinlichkeit, dass auf diesem Weg nicht alle Kontakte korrekt und vollständig durch das Gesundheitsamt ermittelt werden können.

Für die digitale Kontaktdatenerfassung durch Veranstalter wurden zeitnah nach der Einführung dieser Schutzmaßnahme weitere Apps entwickelt – allerdings nicht vom Robert-Koch-Institut, sondern von Unternehmen, darunter die Luca-App. Dieses System wies gegenüber anderen Apps zur Kontaktdatenerfassung Alleinstellungsmerkmale auf. Erstens band es zusätzlich die Gesundheitsämter als Systemnutzer ein, sodass die Kommunikation und die Datenübermittlung zwischen Gesundheitsämtern und Veranstalter direkt über das System erfolgte. Zweitens verfolgten die Betreiber ein besonderes Geschäftsmodell. Kunden waren nicht die Veranstalter, sondern die Gesundheitsämter. Anfang 2021 hatten 13 von 16 Bundesländern Verträge zur Luca-Nutzung mit culture4life abgeschlossen.

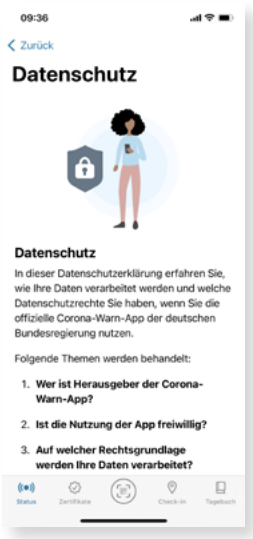
Position der Datenschutzkonferenz

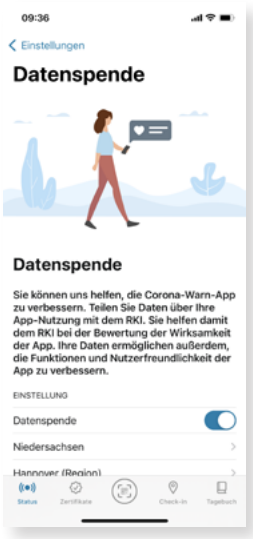
Stellungnahme der DSK: https://t1p.de/Stellungnahme-Kontaktnachverfolgung

Die Datenschutzkonferenz begleitete sehr eng die Entwicklung der digitalen Kontaktnachverfolgung. Ihre erste Stellungnahme zu diesem Thema vom 26. März 2021 „Kontaktnachverfolgung in Zeiten der Corona-Pandemie: Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden“ enthielt neben einer grundsätzlichen Positionierung bereits konkrete Hinweise auf die Datenschutzkonformität der Luca-App. Die DSK betonte, dass eine digitalisierte Kontaktnachverfolgung im Interesse sowohl der effizienten Pandemiebekämpfung als auch des Datenschutzes ist. Denn die Aufsichtsbehörden hatten zuvor sehr viele Beschwerden in Bezug auf die papiergebundene Kontaktnachverfolgung erhalten.

Auch digitale Verfahren zur Verarbeitung von Kontakt- und Anwesenheitsdaten müssen datenschutzkonform betrieben werden. Die DSK befürwortete eine bundesweit einheitliche, datensparsame digitale Infektionsnachverfolgung und forderte den Gesetzgeber auf, hierfür die erforderlichen Vorgaben zu schaffen. In Bezug auf das Luca-System wurde ausgeführt, dass bei zentral betriebenen Diensten generell ein Nachweis der Systemsicherheit unerlässlich und durch die DS-GVO vorgeschrieben ist. Zudem wurde culture4life als Folge der Prüfung der Luca-App durch eine Taskforce der DSK aufgefordert, weitere Anpassungen vorzunehmen, um den Schutz der teilnehmenden Personen weiter zu erhöhen.

Folge der Entscheidung der 13 Länder für das Luca-System waren in vielen Ländern Anpassungen der Corona-Verordnungen. Die Verwendung des Luca-Systems wurde teils verbindlich für die Kontaktnachverfolgung vorgeschrieben, so z. B. in Schleswig-Holstein, teils gegenüber anderen Formen der Kontaktnachverfolgung privilegiert, wie z. B. in Niedersachsen.





Corona-Warn-App als datensparsame Alternative

Aufgrund der starken Fokussierung auf das Luca-System machte die DSK darauf aufmerksam, dass mit der Corona-Warn-App eine datensparsamere Möglichkeit der pseudonymisierten Clustererkennung und Kontaktbenachrichtigung zur Verfügung steht. Hierzu veröffentlichte sie am 29. April 2021 die Entschließung „Chancen der Corona-Warn-App 2.0 nutzen". Darin wurde darauf hingewiesen, dass die CWA seit dem Update auf die Version 2.0 über eine entsprechende Registrierungsfunktion verfügte, die für die Anmeldung an Orten oder bei Veranstaltungen genutzt werden konnte. Durch die unmittelbare Vernetzung der CWA-Nutzerinnen und Nutzer würden Personen, die einem potentiellen Infektionsrisiko ausgesetzt waren, schneller als über die Gesundheitsämter informiert. Die DSK hat sprach daher die Empfehlung aus, die Nutzung der CWA als ergänzende Möglichkeit zur Benachrichtigung potenziell infizierter Personen und zur Clustererkennung in den Konzepten zur Pandemiebekämpfung zu berücksichtigen.

Entschließung zu den Chancen der CWA 2.0: https://t1p.de/CWAnutzen

Zeitgleich mit dieser Entschließung nahm die DSK erneut zu „Kontaktnachverfolgungssystemen – insbesondere zu ‚Luca' der culture4life GmbH" Stellung. Die DSK betonte noch einmal, dass sie die Entwicklung und den datenschutzkonformen Einsatz von digitalen Systemen zur Kontaktnachverfolgung unterstützte. Des Weiteren ging sie auf öffentlich bekanntgewordene Sicherheitsdefizite der Luca-App ein und bestätigte, dass noch weitere Sicherheitsmaßnahmen erforderlich seien, um alle datenschutzrechtlichen Anforderungen zu erfüllen. Abschließend plädierte die DSK erneut dafür, den zur Dokumentation verpflichteten Veranstaltern neben der Nutzung von einer oder mehreren digitalen Anwendungen ihren Gästen auch alternative Möglichkeiten zu eröffnen.

Stellungnahme zu Kontaktnachverfolgungssystemen: https://t1p.de/Kontaktnachverfolgungssysteme

Orientierungshilfe soll Auswahl erleichtern

Um sowohl die Pluralität digitaler Kontaktnachverfolgungssysteme zu fördern als auch den zur Dokumentation verpflichteten Stellen die Systemauswahl zu erleichtern, veröffentlichte die DSK am 29. April 2021 auch die Orientierungshilfe „Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurants- und Geschäftsbesuchen

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

zur Verhinderung der Verbreitung von Covid-19". Diese erläuterte umfassend die Anforderungen an derartige Systeme und ihren Betrieb, die sich aus den gesetzlichen Vorgaben ergeben.

Stellungnahme zur Verantwortlichkeit bei Kontaktnachverfolgungssystemen: https://t1p.de/Stellungnahme-Verantwortlichkeit-Kontaktnachverfolgung

Die fünfte und letzte Veröffentlichung der DSK im Jahr 2021 zum Thema Kontaktnachverfolgung war die „Stellungnahme zur Verantwortlichkeit bei der Nutzung von Kontaktnachverfolgungssystemen wie der Luca App" vom 21. Mai 2021. Aufgrund der Vielzahl von Beteiligten beim Einsatz des Luca-Systems – die culture4life GmbH als Anbieter und Betreiber, Veranstalter, Besucher von Veranstaltungen und die Gesundheitsämter – tauchte immer wieder die Frage nach der datenschutzrechtlichen Verantwortlichkeit auf. Die DSK wies deshalb in der Stellungnahme darauf hin, dass sie die Gestaltung des Verhältnisses zwischen App-Anbieter und den Veranstaltern sowohl als Auftragsverarbeitung als auch als gemeinsame Verantwortlichkeit datenschutzrechtlich für vertretbar hält. Zudem wurde betont, dass Datenverarbeitungen durch die Gesundheitsämter, denen gesetzliche Regelungen zu Grunde liegen, eine gesonderte eigene Verantwortlichkeit begründen.

Datenschutz von Anfang an einplanen

Die Corona-Pandemie hat in sehr vielen Bereichen als Motor für die Digitalisierung gewirkt. Am Beispiel der Kontaktnachverfolgung zeigen sich deutlich die Vorteile von digitalen Lösungen, um effizient und mit möglichst geringem Aufwand komplexe Datenverarbeitungsvorgänge mit mehreren unterschiedlichen Beteiligten umzusetzen. Allerdings wird der Datenschutz bei Digitalisierungsmaßnahmen leider häufig nicht von Anfang an im wünschenswerten Umfang mit eingeplant. Der konkrete Vergleich der CWA mit der Luca-App zeigt – ungeachtet des teils nicht deckungsgleichen Funktionsumfangs – wie vorteilhaft es ist, den Datenschutz bereits bei der Konzeption und Entwicklung datenverarbeitender Systeme zu berücksichtigen.

An der Entwicklung der CWA waren von Beginn an Datenschützer beteiligt. Diese haben letztlich die Systemarchitektur der dezentralen Datenverarbeitung durchgesetzt und damit die Basis für eine datenschutzkonforme Anwendung gelegt. Bei der Entwicklung der Luca-App standen die Funktionalitäten im Fokus, obschon datenschutzrechtliche Anforderungen berücksichtigt worden sind. Von den Aufsichtsbehörden datenschutzrechtlich geprüft wurde die App jedoch erst, nachdem sie bereits breitflächig eingesetzt wurde. Datenschutzrechtlich erforderliche Anpassungen können zu so einem späten Zeitpunkt nur noch mit hohem Aufwand vorgenommen und wesentliche Konstruktionsansätze teilweise gar nicht mehr verändert werden. Der von der DS-GVO eingeführte Ansatz „Privacy by Design" sollte daher bei allen Entwicklungsprozessen so früh wie möglich beherzigt werden. Zudem würde ich mich freuen, wenn die Ministerien mich bei so wichtigen und datenschutzrelevanten Entscheidungen wie dem Abschluss von Kooperationsvereinbarungen mit Unternehmen zum flächendeckenden Einsatz digitaler Anwendungen in Niedersachsen frühzeitig beteiligen würden.

Abfrage der 3G-Daten

Entschließung zur Impfdatenverarbeitung: https://t1p.de/Impfdatenverarbeitung

Bei den 3G-Daten handelt es sich um Gesundheitsdaten, deren Verarbeitung grundsätzlich gemäß Art. 9 Abs. 1 DS-GVO untersagt ist. Sie dürfen nur in gesetzlich ausdrücklich geregelten Ausnahmefällen verarbeitet werden.

Mit ihrer Entschließung vom 29. März 2021 „Coronavirus: Impfnachweis, Nachweis negativen Testergebnisses und Genesungsnachweis in der Privatwirtschaft und im Beschäftigungsverhältnis gehören gesetzlich geregelt!“ stellte dies die DSK auch im Zusammenhang mit den 3G-Daten fest. Zum damaligen Zeitpunkt fehlten weitestgehend gesetzliche Regelungen zur Nachweispflicht einer Impfung, einer Genesung bzw. eines negativen Tests, um den Zugang zu privatwirtschaftlichen Veranstaltungen oder Einrichtungen zu ermöglichen. Dies galt auch für Beschäftigte gegenüber ihren jeweiligen Arbeitgeberinnen und Arbeitgebern. Die Aufsichtsbehörden erreichten jedoch fortlaufend Beratungsanfragen von Arbeitgeberinnen und Arbeitgebern, die Gesundheitsdaten wie die Körpertemperatur oder den Impfstatus von Beschäftigten erheben und verarbeiten wollten.

Abfrage des Impfstatus im Beschäftigungsverhältnis

Im Zusammenhang mit der Corona-Pandemie habe ich allgemeine Hinweise zur Verarbeitung von Gesundheitsdaten Beschäftigter bereits in meinem Tätigkeitsbericht 2020 erteilt.

Außer in gesetzlich ausdrücklich geregelten Fällen – wie beispielsweise für Arbeitgeberinnen und Arbeitgeber im Gesundheitsbereich gemäß § 23 und § 23a des Infektionsschutzgesetzes (IfSG) – bestand für weitere Arbeitgeberinnen und Arbeitgeber zunächst keine Rechtsgrundlage, die eine Verarbeitung der 3G-Daten ihrer Beschäftigten generell zuließ. Auch die DSK stellte in ihrem Beschluss „Verarbeitung des Datums ‚Impfstatus´ von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber“ vom 19. Oktober 2021 fest, dass eine ausdrückliche gesetzlichen Ermächtigung für die Verarbeitung des Impfstatus notwendig ist.

Beschluss Verarbeitung des Impfstatus durch Arbeitgeber: https://t1p.de/Impfstatusverabreitung-durch-Arbeitgeber

Zwischenzeitlich erließ der Bundesgesetzgeber § 28b IfSG, der die Verarbeitung von 3G-Daten durch Arbeitgeberinnen und Arbeitgeber im Rahmen von Zugangskontrollen zu Betriebsstätten regelt. Dennoch bleibt die rechtskonforme Verarbeitung von 3G-Daten der Beschäftigten für Arbeitgeberinnen und Arbeitgeber eine Herausforderung. Denn diese Regelung ist stark auslegungsbedürftig. Eine Unterstützung für Verantwortliche und Betroffene bietet die Anwendungshilfe „Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie“ der DSK vom 20. Dezember 2021. Hiermit sollte einerseits den Verantwortlichen eine datenschutzkonforme Verarbeitung erleichtert werden. Andererseits sollte es die Anwendungshilfe den Betroffenen erleichtern, die Rechtmäßigkeit der Verarbeitung ihrer Daten zu überprüfen.

Anwendungshilfe der DSK: https://t1p.de/FAQ-Verarbeitung-Impfstatus

Es ist abzusehen, dass die gesetzlichen Regelungen – wie bisher – häufig und kurzfristig der pandemischen Lage angepasst werden. Viele dieser Regelungen betreffen die Verarbeitung von personenbezogenen Daten. Auch im weiteren Verlauf der Corona-Pandemie wird die datenschutzkonforme Verarbeitung von personenbezogenen Daten von Betroffenen, insbesondere der Beschäftigten, deshalb für die Verantwortlichen eine Herausforderung bleiben. Ich werde sie bei der datenschutzkonformen Anwendung der Regelungen weiterhin unterstützen sowie die Beschwerden der Betroffenen prüfen und gegebenenfalls aufsichtsrechtliche Maßnahmen treffen.

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 (AK) Beschäftigtendatenschutz. Schwerpunktthema im Jahr 2021 war die Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie.

Aufgabe des AK Beschäftigtendatenschutz ist es, einheitliche Positionen aller Aufsichtsbehörden zu datenschutzrechtlichen Fragen im Beschäftigtenkontext zu erarbeiten und hierzu Entscheidungen der DSK vorzubereiten.

Die turnusmäßige Sitzung des AK im Januar 2021 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. So wurden im Berichtszeitraum beispielsweise Herausforderungen im Zusammenhang mit dem Umgang von Führungszeugnissen erkannt, unter anderem im Hinblick auf die Möglichkeit der Einbindung von sogenannten „Treuhändern" für deren Vorab-Prüfung, sowie im Hinblick auf die Erforderlichkeit der Speicherung von Kopien der Zeugnisse in Personalakten.

Besondere Veröffentlichungen der DSK

Im Zusammenhang mit der Corona-Pandemie befasste sich der AK mit der Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie. Eine bundesweite und länderübergreifende Positionierung gestaltete sich aufgrund der nach dem Infektionsschutzgesetz zu beachtenden unterschiedlichen bundes- und landesrechtlichen Regelungen und – damit verbunden – unterschiedlichen Entscheidungen von Gerichten nicht immer leicht.

Beschluss der DSK: https://t1p.de/beschluss-impfstatus

Dennoch konnte der AK Beschäftigtendatenschutz den Beschluss „Verarbeitungen des Datums ‚Impfstatus' von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber" vom 19. Oktober 2021 für die DSK erarbeiten. Darin wurden die zu diesem Zeitpunkt gültigen Rechtsgrundlagen für eine Verarbeitung zusammengefasst und rechtlich bewertet.

Anwendungshilfe der DSK: https://t1p.de/oh-corona

Zudem veröffentlichte die DSK am 20. Dezember 2021 nach Vorarbeit des AK Beschäftigtendatenschutz die Anwendungshilfe „Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusam-

menhang mit der Corona-Pandemie". Es handelt sich um eine umfangreiche Anwendungshilfe für den praktischen Vollzug. Die Fallgestaltungen beziehen sich auf die Verarbeitung von Daten der Beschäftigten, einschließlich ihrer Gesundheitsdaten durch Arbeitgeberinnen und Arbeitgeber. Die Ausführungen gelten auch für Beschäftigte im öffentlichen Bereich, soweit für diese nicht besondere Regelungen vorrangig anzuwenden sind.

Ausblick

Leider lag bis zum Redaktionsschluss der avisierte Abschlussbericht des im letzten Tätigkeitsbericht erwähnten Beirats „Beschäftigtendatenschutz" des Bundesministeriums für Arbeit und Soziales zur Frage, ob es eines Beschäftigtendatenschutzgesetzes bedarf, noch nicht vor. Der AK Beschäftigtendatenschutz wird sich diesem wichtigen Thema im Jahre 2022 widmen.

E.3. Bericht aus dem Arbeitskreis Versicherungswirtschaft

In der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) führe ich den Vorsitz des Arbeitskreises (AK) Versicherungswirtschaft. Die teilnehmenden Aufsichtsbehörden beraten in dem AK über Fragen, die sich im Zuge der datenschutzrechtlichen Aufsicht über Versicherungsunternehmen stellen. Ziel dieser Beratungen ist es, eine einheitliche Aufsichtspraxis in Deutschland zu gewährleisten.

Die beaufsichtigten Versicherungsunternehmen werden zu den Rechtsauffassungen der Aufsichtsbehörden regelmäßig über den Gesamtverband der Deutschen Versicherungswirtschaft angehört und erhalten Gelegenheit, datenschutzrechtliche Themen vorzutragen und mit den Datenschutzaufsichtsbehörden zu erörtern, die in der Praxis der Versicherungsunternehmen zu Rechtsunsicherheit führen.

Verarbeitung von Daten in der Kranken- und Lebensversicherung

Im Berichtszeitraum lag ein Schwerpunkt auf der Verarbeitung von besonderen Kategorien personenbezogener Daten – insbesondere Gesundheitsdaten – im Rahmen der Kranken- und Lebensversicherung. Diese Daten unterliegen nach Art. 9 Datenschutz-Grundverordnung (DS-GVO) einem besonderen Schutz. Neben den Voraussetzungen des Art. 6 Abs. 1 DS-GVO müssen die in Art. 9 DS-GVO genannten Voraussetzungen erfüllt sein, bevor ein Versicherungsunternehmen Gesundheitsdaten verarbeiten darf.

Weil Art. 9 Abs. 2 DS-GVO im Gegensatz zu Art. 6 Abs. 1 lit. b DS-GVO keine Rechtsgrundlage für eine Verarbeitung zur Begründung, Durchführung oder Beendigung eines Vertrages enthält, ist es notwendig, von den Versicherungsnehmern datenschutzrechtliche Einwilligungen einzuholen. Der Gesamtverband der Deutschen Versicherungswirtschaft hat hierzu Mustereinwilligungserklärungen entworfen, die durch einen Unterarbeitskreis der DSK auf ihre Vereinbarkeit mit den Vorgaben der DS-GVO für wirksame Einwilligungen geprüft und mit der Versicherungswirtschaft diskutiert wurden. Die Ergebnisse des Unterarbeitskreises wurden anschließend auf der Sitzung des Arbeitskreises Versicherungswirtschaft im November 2021 umfassend beraten. Im Berichtszeitraum konnte dennoch die Prüfung der Mustererklärungen noch nicht vollständig abgeschlossen werden. Sie wird daher im Jahr 2022 fortgesetzt.

E.4. Orientierungshilfe zum TTDSG: Neue Spielregeln für das Webtracking

Die Einführung des Telekommunikations-Telemediengesetzes (TTDSG) sorgte zum Ende des Jahres 2021 für einige Aufregung bei Betreibern von Webseiten und Apps. Neben der allgemeinen Frage, wie das konkrete Verhältnis zwischen TTDSG und Datenschutz-Grundverordnung (DS-GVO) ist, wirft der § 25 TTDSG zu Cookies und Tracking-Methoden auf Webseiten und in Apps zahlreiche Fragen auf. Die Aufsichtsbehörden geben hierauf Antworten in einer neuen Orientierungshilfe.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) veröffentlichte am 21. Dezember 2021 eine neue Fassung der Orientierungshilfe für Anbieterinnen und Anbieter von Telemedien. Das Papier bietet Betreiberinnen und Betreibern von Webseiten, Apps oder Smarthome-Anwendungen konkrete Hilfestellungen bei der Umsetzung der neuen Vorschriften des TTDSG. Zudem vermittelt die Orientierungshilfe betroffenen Bürgerinnen und Bürgern ein besseres Bild der rechtlichen Rahmenbedingungen.

Orientierungshilfe für Anbieter von Telemedien: https://t1p.de/OH-Telemedien

Seit dem 1. Dezember 2021 regelt das TTDSG zusätzlich zum Datenschutz bei Telekommunikations- und Telemediendiensten den Schutz der Privatsphäre bei der Nutzung von Endgeräten. Daraus ergeben sich insbesondere praxisrelevante Auswirkungen auf den Einsatz von Cookies und ähnlichen Technologien. Mit dem TTDSG hat der Bundesgesetzgeber nach über einem Jahrzehnt Verzögerung nun die Vorgaben der europäischen E-Privacy-Richtlinie in der Fassung von 2009 – die sogenannte Cookie-Richtlinie – in nationales Recht umgesetzt.

Die Orientierungshilfe gliedert sich in drei Teile. Im ersten Teil finden sich allgemeine Ausführungen zur neuen Rechtslage, zu den Adressaten des Gesetzes und dem räumlichen Anwendungsbereich des TTDSG. Es folgt eine Abgrenzung dieses spezifischen Datenschutzgesetzes zur DS-GVO.

Schutz der Privatsphäre in Endeinrichtungen

Der zweite Teil behandelt sehr ausführlich den Schutz der Privatsphäre in Endeinrichtungen, der in § 25 TTDSG geregelt ist. Es werden der Grundsatz der

Einwilligungsbedürftigkeit des Speicherns und Auslesens von Informationen auf bzw. aus den Endgeräten der Nutzerinnen und Nutzer, die gesetzlichen Anforderungen an die Einwilligung sowie die in § 25 Abs. 2 TTDSG vorgesehenen Ausnahmen von der Einwilligungspflicht erläutert.

Bei Telemedien ist die Ausnahme von diesem Einwilligungserfordernis sehr eng auf Fälle begrenzt, in denen das Speichern und Auslesen der Informationen unbedingt erforderlich ist, damit ein ausdrücklich von Nutzerinnen und Nutzern gewünschter Telemediendienst zur Verfügung gestellt werden kann. In der Orientierungshilfe finden sich maßgebliche Kriterien, wie der entsprechende Nutzerwunsch festgestellt werden kann. Aus dem Aufruf einer Webseite kann nicht bereits geschlossen werden, dass der Nutzer oder die Nutzerin alle Funktionen eines Telemediendienstes wünscht. Erst wenn die jeweiligen Einzelfunktionen konkret in Anspruch genommen werden, zum Beispiel indem ein Kontaktformular ausgefüllt oder bei einem Online-Shop ein Produkt in den Warenkorb gelegt wird, ist der Nutzungswunsch anzunehmen. Das Speichern und Auslesen der Informationen auf bzw. aus den Endgeräten

darf nur erfolgen, soweit es für die ausdrücklich gewünschten Funktionen des Telemediendienstes unbedingt erforderlich ist. Aus dieser differenzierten Betrachtung folgt, dass auch wenn die Voraussetzungen der Ausnahme vorliegen, Cookies und Drittdienste jeweils erst bei bestimmten Nutzungsvorgängen auf der Webseite aktiv werden dürfen und nicht bereits beim Aufruf der Startseite.

Vergleich zur bisherigen Rechtslage

Ein ergänzender Hinweis bezieht sich auf einen Vergleich mit der bisherigen Rechtslage. Bei der Prüfung, ob ausnahmsweise eine Einwilligung entbehrlich ist, ist zu beachten, dass die Voraussetzungen sich wesentlich vom in Art. 6 Abs. 1 lit. f. DS-GVO vorgegebenen Kriterium des berechtigten Interesses unterscheiden. Bis zum 30. November 2021 wurde ein das Nutzerinteresse überwiegendes berechtigtes Interesse der verantwortlichen Betreiber von Webseiten von den Aufsichtsbehörden unter engen Voraussetzungen als mögliche Rechtsgrundlage angesehen. Eine bisherige Interessenabwägung nach der DS-GVO erfüllt jedoch nicht automatisch die engen Voraussetzungen der Ausnahmeregelung im TTDSG. Zur Umsetzung der neuen Rechtslage ist es daher beispielsweise nicht ausreichend, wenn lediglich die Bezeichnungen der Rechtsgrundlagen in einer Datenschutzerklärung auf der Webseite oder in der App ausgetauscht werden.

Dem Einsatz von Cookies und Tracking-Methoden schließt sich regelmäßig eine Verarbeitung personenbezogener Daten an. Daher werden im dritten Teil der Orientierungshilfe die Voraussetzungen der Rechtmäßigkeit dieser nachgelagerten Verarbeitungsprozesse nach der DS-GVO dargestellt. Dieser dritte Teil entspricht weitgehend der Vorversion der Orientierungshilfe.

Konsultationsverfahren zur Weiterentwicklung

Pressemitteilung zum Start der Konsultation: https://t1p.de/konsultation-oh

Die DSK plant, zeitnah auch eine englische Fassung der Orientierungshilfe zur Verfügung zu stellen. Zudem wurde am 14. Januar 2022 ein öffentliches Konsultationsverfahren zur neuen Fassung der Orientierungshilfe eingeleitet. Es gab Vertreterinnen und Vertretern aus Politik, Wirtschaft, Wissenschaft, Gesellschaft und Verwaltung Gelegenheit, bis zum 15. März 2022 zur Orientierungshilfe Stellung zu nehmen. Das Konsultationsverfahren dient der Überprüfung und ggf. der Fortentwicklung der Orientierungshilfe, berührt aber nicht ihre Geltung und Anwendung in der Praxis der Aufsichtsbehörden.

Es freut mich sehr, dass es der DSK so zeitnah mit dem Inkrafttreten des TTDSG gelungen ist, mit der Orientierungshilfe eine wertvolle Anwendungshilfe für öffentliche und nicht öffentliche Stellen zur Verfügung zu stellen. Das Konsultationsverfahren sehe ich als Chance, ein erstes und unmittelbares Feedback aus der Praxis einzuholen und gegebenenfalls verbleibende Unklarheiten und Unsicherheiten aufzudecken.

E.5. Anpassung der Orientierungshilfe zu Schutzmaßnahmen beim E-Mail-Versand

Verantwortliche müssen Risiken, die durch die Übermittlung personenbezogener Daten per E-Mail für die Rechte der Betroffenen entstehen, mit angemessenen Maßnahmen soweit mindern, dass ein dem Risiko angemessenes Schutzniveau gewährleistet ist. Eine Orientierungshilfe der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bietet hierfür Unterstützung.

Die seit März 2020 vorliegende Orientierungshilfe (DSK) zeigt auf, welche Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mail-Nachrichten durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche E-Mail-Diensteanbieter auf dem Transportweg zu erfüllen sind. Diese richten sich nach den Vorgaben des Art. 5 Abs. 1 lit. f, 25 und Art. 32 Abs. 1 Datenschutz-Grundverordnung (DS-GVO).

Änderungsbedarf im Berichtsjahr 2021

Orientierungshilfen bedürfen auch immer der evaluierenden Beobachtung, ob sie im Datenschutzalltag anwendbar und hilfreich sind. Durch diese kritische Hinterfragung hat sich im Berichtszeitraum Änderungsbedarf an der Orientierungshilfe zum E-Mail-Versand ergeben.

Aktualisierte Orientierungshilfe E-Mail-Versand: https://t1p.de/oh-mail

So ist in Niedersachsen festzustellen, dass bei IT-Dienstleistern aus Rücksicht auf verschiedene geforderte Funktionalitäten auf Mailservern und Endgeräten die empfehlenswerte konsequente Umsetzung der Transportverschlüsselung beim E-Mail-Verkehr hinausgezögert wurde. Auch der Beauftragte für Informationssicherheit beim Niedersächsischen Innenministerium beklagt diesen Umstand. Im Rahmen der Beratungen gegenüber dem IT-Verantwortlichen der Landesregierung und dem Niedersächsischen IT-Planungsrat habe ich die Notwendigkeit dieses Standards zum Ausdruck gebracht, um eine grundlegende Schutzbasis für die Vertraulichkeit des E-Mail-Verkehrs und der Inhaltsdaten zu gewährleisten.

Ein zweiter Aspekt ist die Einhaltung grundlegender Prinzipien der DS-GVO. Aus meiner Aufsichts- und Beratungspraxis heraus ist es im Alltag erforderlich, mit der Orientierungshilfe keine strikte Kategorisierung von Beispielfällen bzw. Fallgruppen festzulegen, sondern zunächst auf die durch Artikel 5, 24, 25 und 32 DS-GVO geforderte risikobasierte Einzelfallprüfung hinzuweisen. Eine Kategorienbildung, wie sie in der Orientierungshilfe für Fallgruppen dargestellt ist, gibt zwar eine Leitplanke, muss jedoch den Prüfspielraum belassen, den jeder Verantwortliche nach der DS-GVO ausüben muss. Deshalb wird bereits im ersten Kapitel der OH ein Hinweis gegeben, wonach die Verantwortlichen und Auftragsverarbeiter verpflichtet sind, die Besonderheiten ihrer Verarbeitungen, zu berücksichtigen, die ggf. in abweichenden Anforderungen resultieren können. Auf diesen Abwägungsprozess kann ein Verantwortlicher nicht verzichten, weil eine strikte Anwendung von Blaupausen den individuellen Besonderheiten in der Risikobewertung bestimmter Fälle nicht gerecht werden würde.

Elektronische Kommunikation mit Justiz und Behörden

Eine Besonderheit im E-Mail-Verkehr sind die neuen Postfachkonzepte auf sicheren Übermittlungswegen: So soll mit dem „elektronischen Bürger- und Organisationen-Postfach" (eBO) und dem Steuerberaterpostfach die elektronische Kommunikation mit Justiz und Behörden deutlich an Fahrt aufnehmen. Die Einführung des eBO ist bereits zum 1. Januar 2022, das besondere elektronische Steuerberaterpostfach zum 1. Januar 2023 geplant. Zudem ha-

ben Behörden, Körperschaften und Anstalten des öffentlichen Rechts sichere Übermittlungswege verpflichtend zu eröffnen.

Im Rahmen der Überprüfung der Orientierungshilfe wurde über eine Änderung beraten, wie die Regelungen im Berufsrecht und Strafrecht im Verhältnis zur DS-GVO stehen. Hierzu hat der Arbeitskreis (AK) Technik der DSK eine Änderung vorgeschlagen, in der dieses Verhältnis genauer beschrieben und in der die Ausführungen in Abschnitt 4.2.3 neu gefasst wurden. Diese Änderungen wurden von der DSK am 16. Juni 2021 angenommen und beschlossen. Die geänderte Fassung ist veröffentlicht.

Bewusster Verzicht auf Schutzmaßnahmen?

Eine weitere Frage war, ob Betroffene bewusst auf technische und organisatorische Maßnahmen wie etwa eine Verschlüsselung verzichten können. Die DSK fasste am 24. November 2021 den folgenden Vier-Punkte-Beschluss mit dem Titel „Zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO auf ausdrücklichen Wunsch betroffener Personen:

Beschluss zum Verzicht auf TOM: https://t1p.de/verzicht-tom

1. Die vom Verantwortlichen nach Art. 32 DSGVO vorzuhaltenden technischen und organisatorischen Maßnahmen beruhen auf objektiven Rechtspflichten, die nicht zur Disposition der Beteiligten stehen.
2. Ein Verzicht auf die vom Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen oder die Absenkung des gesetzlich vorgeschriebenen Standards auf der Basis einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ist nicht zulässig.
3. Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen, eigeninitiativen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet.
4. Kapitel V der DSGVO (Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen) bleibt hiervon unberührt.

Die Praxisrelevanz dieser wichtigen Orientierungshilfe wird weiterhin in meiner täglichen Aufsichts- und Beratungsarbeit darauf überprüft, ob Anpassungen und Verbesserungen notwendig sind.

E.6. Auftragsverarbeitung bei Microsoft Office 365 weiterhin nicht DS-GVO-konform

In meinem Tätigkeitsbericht 2020 habe ich ausführlich über die datenschutzrechtlichen Herausforderungen beim Einsatz von Microsoft Office 365-Produkten berichtet. Im Jahr 2021 wurden die Gespräche zwischen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eingesetzten Arbeitsgruppe und Microsoft fortgesetzt; gleichzeitig erreichten mich weiterhin viele Anfragen von Verantwortlichen zum datenschutzkonformen Einsatz.

Angesichts der Anfragen der Verantwortlichen prüfte ich (parallel zur Fortführung der Gespräche zwischen Microsoft und der DSK) die Standard-Datenschutzbestimmungen (Data Protection Addendum „DPA") von Microsoft aus dem Dezember 2020 daraufhin, ob die von der DSK 2020 kritisierten Punkte eine Verbesserung erfahren hatten. Leider konnte ich in den meisten Punkten keine wesentlichen Verbesserungen feststellen.

Noch immer erfüllen die Office 365 Produkte Anforderungen der Datenschutz-Grundverordnung (DS-GVO) nicht vollständig. Mängel bestehen insbesondere bei:

- den Vorgaben zur Auftragsverarbeitung gem. Art. 28 DS-GVO sowie
- der Transparenz und Abgrenzung bei der Verwendung von Daten durch Microsoft zu eigenen Zwecken.

Ich kann nachvollziehen, dass diese Situation für die Verantwortlichen unbefriedigend ist. Jedoch liegt die Verantwortung dafür nicht beim Datenschutz. Stattdessen sind die Verantwortlichen gefordert, sich mit der Datenverarbeitung, die im Rahmen der Nutzung bestimmter Produkte geschieht, genau zu befassen und ggf. nach datenschutzfreundlichen Alternativen zu suchen. Gleichzeitig ist Microsoft gefordert, auf die Bedürfnisse des europäischen Marktes einzugehen, wenn die Microsoft-Produkte in der EU Absatz finden sollen. Umso bedauerlicher ist es, dass Microsoft die Gesprächsangebote der DSK offenbar nicht dazu genutzt hat, um in der nächsten DPA-Fassung die festgestellten Mängel zu beheben.

Microsoft muss besser auf Gegebenheiten des europäischen Marktes eingehen

Am 15. September 2021 veröffentlichte Microsoft ein neues DPA, mit welchem ich mich ebenfalls befassen werde. Gleichzeitig werden auch die Konsequenzen des „Schrems II"-Urteils des Europäischen Gerichtshofs und die Frage der Übermittlung von Telemetriedaten bei der Beurteilung der Einsatzfähigkeit von Microsoft-Produkten eine wesentliche Rolle spielen.

E.7. Zertifizierung DS-GVO-konformer Datenverarbeitung steht kurz bevor

Eine der wesentlichsten Neuerungen der im Jahr 2018 in Kraft getretenen DS-GVO steht kurz davor, nun endlich zur Geltung zu kommen. Mit der datenschutzrechtlichen Zertifizierung können sich Verantwortliche zukünftig bestätigen lassen, dass personenbezogene Daten im Rahmen ihrer digitalen Produkte und Dienstleistungen datenschutzkonform verarbeitet werden. Diese Transparenz wird Vertrauen schaffen: bei den Verantwortlichen, bei Betroffenen und nicht zuletzt den Datenschutzaufsichtsbehörden, die die verantwortlichen Stellen kontrollieren.

Tätigkeitsbericht 2020: https://t1p.de/2020-tb

Im vorausgegangenen Tätigkeitsbericht habe ich angekündigt, dass die Datenschutzaufsichtsbehörden des Bundes und der Länder an einem Anforderungskatalog für Zertifizierungsprogramme arbeiten, der die grundsätzlichen Anforderungen an eine Programmprüfung aus der Norm EN-ISO/IEC 17067/2013 ergänzt.

Eine Programmprüfung ist einer Akkreditierung vorgeschaltet. Wenn sich eine Stelle als datenschutzrechtliche Zertifizierungsstelle akkreditieren lassen möchte, muss sie zunächst ihr Zertifizierungsprogramm einer solchen Prüfung unterziehen.

Akkreditierungsprozess im Überblick: https://t1p.de/akkreditierungsprozess

Im Rahmen der 101. Datenschutzkonferenz vom 28. bis 29. April 2021 wurden die „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ verabschiedet. Dieses Dokument bildet zum einen eine gemeinsame Grundlage für alle deutschen Aufsichtsbehörden, um eine möglichst einheitliche Bewertung von Zertifizierungskriterien im Sinne des Art. 42 Abs. 5 DS-GVO in Deutschland zu erreichen. Zum anderen hilft es den Programmeignern und den Zertifizierungsstellen bei der Erstellung ihrer Dokumente (insbesondere im Rahmen einer Programmprüfung) als Orientierung.

Anforderungen an Zertifizierungsprogramme: https://t1p.de/Zertifizierungsprogramme

Die „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ umfassen in ihrer ersten Fassung konkrete Prüfkriterien zu den folgenden Artikeln der DS-GVO: Art. 5, 6, 25, 28, 30, 32, 33, 34, 35. Dabei wurde zu den einzelnen Artikeln nicht nur dargestellt, was genau die Zertifizierungsstelle prüfen muss, sondern auch mit welchen Prüfmethoden. Erste pauschale Anforderungen finden sich ferner in Bezug auf die Betroffenenrechte und den Drittlandtransfer. Diese werden in den Folgefassungen weiter vertieft.

Darüber hinaus werden in die Folgefassungen des Dokuments noch die Darstellung weiterer Artikel der DS-GVO (wie z. B. Art. 26) inklusive der passenden Prüfmethoden sowie die Erfahrungen der Aufsichtsbehörden aus der Akkreditierungspraxis einfließen.

Ich freue mich darüber, dass ein weiterer wichtiger Meilenstein für die Akkreditierungs- und Zertifizierungspraxis erreicht wurde und möchte potenzielle Zertifizierungsstellen ermutigen, sich um eine Akkreditierung zu bemühen.

E.8. Ergebnisse der Evaluierung des Bundesdatenschutzgesetzes

Im Jahr 2021 wurde die erste Evaluierung des neuen Bundesdatenschutzgesetzes seit Inkrafttreten der DS-GVO durchgeführt. Insgesamt zeigt sich das Bundesministerium des Innern, für Bau und Heimat (BMI) in seinem Evaluierungsbericht eher verhalten und sieht nur punktuell Prüfungs- oder Änderungsbedarf. Ich hätte mir erhofft, dass der Bund deutlich mehr Empfehlungen der Aufsichtsbehörden aufgreift und die Rechtsdurchsetzung im Datenschutzrecht verbessert.

Ministerium verschickt Fragebögen

Flankierend zur DS-GVO ist am 25. Mai 2018 auch das neue Bundesdatenschutzgesetz (BDSG) in Kraft getreten. Die Neufassung wurde mit dem Artikelgesetz zur Anpassung des Datenschutzrechts an die DS-GVO und zur Umsetzung der JI-Richtlinie verabschiedet. Im Zuge dessen wurde eine Evaluierung vorgesehen[1], die im November 2020 durch das BMI mit der Versendung von Fragebögen an Datenschutzaufsichtsbehörden sowie Verbände und Institutionen eingeleitet wurde. Ziel der Evaluierung war es, die Zweckmäßigkeit, Praktikabilität und Normenklarheit des BDSG zu überprüfen.

Stellungnahmen der Aufsichtsbehörden

Stellungnahme der DSK: https://t1p.de/Evaluierung-BDSG

Die Datenschutzkonferenz (DSK) erteilte auf ihrer 100. Sitzung am 25. und 26. November 2020 ihrem Arbeitskreis Grundsatz den Auftrag, eine Evaluierungs-Stellungnahme zu erarbeiten. Der Arbeitskreis gründete hierfür wiederum eine Unterarbeitsgruppe, in der auch meine Behörde maßgeblich mitwirkte und eine Berichterstatterrolle übernahm. Die Arbeiten mündeten schließlich in der gemeinsamen DSK-Stellungnahme vom 2. März 2021. Flankierend hierzu gab eine Mehrheit der Landesdatenschutzaufsichtsbehörden eine von meiner Behörde koordinierte gemeinsame Stellungnahme mit zusätzlichen Anmerkungen aus Ländersicht ab. Außerdem hatten die Aufsichtsbehörden des Bundes und der Länder Mitte des vergangenen Jahres Gelegenheit, in einer gemeinsamen Besprechung mit dem BMI und dem Bundesministerium der Justiz und für Verbraucherschutz ihre Sichtweise zu ausgewählten Punkten darzustellen.

BMI sieht nur wenig Änderungs- oder Prüfungsbedarf

Im Oktober 2021 legte das BMI seinen Evaluierungsbericht vor. Das Ministerium kam zu dem Ergebnis, dass die überwiegende Zahl der Regelungen

1 BT-Drucksache 18/11325, S. 78.

Stellungnahme des BMI: https://t1p.de/StellungnahmeBMI

des BDSG als sachgerecht, praktikabel und normenklar angesehen werden könne. Die meisten der eingegangenen Rückmeldungen hätten sich aus Sicht des BMI jeweils nur auf wenige Vorschriften bezogen und zu einem Großteil der Regelungen weder Verständnis- noch Anwendungsschwierigkeiten dargelegt. In der Gesamtschau sah das BMI nur punktuellen Änderungsbedarf in Bezug auf bestimmte gesetzliche Klarstellungen oder redaktionelle Verbesserungen. Eine Reihe inhaltlicher Änderungsvorschläge solle weiter geprüft werden, etwa die Zuerkennung von weiteren Befugnissen der Aufsichtsbehörden im Bußgeldverfahren oder eine Änderung der Regelung zur Videoüberwachung öffentlich zugänglicher Räume durch nichtöffentliche Stellen gemäß § 4 BDSG. Für diese verbleibt in der jetzigen Form aufgrund des vorrangig anwendbaren Art. 6 Abs. 1 Buchstabe f DS-GVO kein Raum.

Defizite beim Vollzug bleiben unangetastet

Eine Vielzahl von Änderungsvorschlägen der Aufsichtsbehörden wurde leider abgelehnt. Dazu zählt die von der DSK empfohlene Korrektur in § 41 Abs. 1 S. 2 BDSG, dass §§ 30, 130 des Gesetzes über Ordnungswidrigkeiten keine Anwendung finden, um die von der DS-GVO voraus-

gesetzte uneingeschränkte Verbandshaftung und den Anwendungsvorrang des Unionsrechts zu verdeutlichen (siehe hierzu auch F.3, S. 55). Mit der Frage der Nichtanwendbarkeit des § 30 OWiG wird sich stattdessen demnächst der EuGH befassen müssen.[2] Ebenso abgelehnt wurde die Forderung der DSK, in § 43 Abs. 3 BDSG vorzusehen, dass gegen Behörden und öffentliche Stellen Geldbußen verhängt werden dürfen. Die Begründung von BMI, dass die bestehenden Abhilfebefugnisse in Form der Verwarnung, Beanstandung, Anweisung oder der Beschränkung oder dem Verbot der Verarbeitung ausreichend seien, überzeugt mich jedoch nicht, weil diese Abhilfebefugnisse nicht mit Zwangsmaßnahmen gegenüber öffentlichen Stellen durchgesetzt werden können. Auch das hatte die DSK zu Recht moniert, das BMI sieht jedoch auch diesbezüglich keinen Änderungsbedarf, weil Behörden ihren öffentlich-rechtlichen Verpflichtungen auch ohne Anwendung von Zwangsmitteln nachkämen. Diese Ansicht kann ich jedoch nicht uneingeschränkt teilen, vielmehr hat die aufsichtsbehördliche Praxis meines Erachtens gezeigt, dass ein Bedarf besteht, Abhilfemaßnahmen auch im öffentlichen Bereich durchsetzen zu können.

Beschäftigtendatenschutz und Institutionalisierung der DSK bleiben weiter offen

In der Gesamtschau zeigte sich das BMI bei seiner Analyse eher zurückhaltend und will überwiegend am Status quo festhalten oder die weitere Entwicklung abwarten. Das gilt namentlich im Hinblick auf das seit Jahren geforderte Beschäftigtendatenschutzgesetz, für welches das BMI derzeit keinen zwingenden Bedarf sieht. Hier bleibt abzuwarten, zu welchen Ergebnissen der vom Bundesministerium für Arbeit und Soziales eingesetzte Beirat zum Beschäftigtendatenschutz kommen wird.

Außerdem hätte ich mir gewünscht, dass das BMI die Evaluierung zum Anlass nimmt, die von mir schon mehrfach geforderte Institutionalisierung der Datenschutzkonferenz voranzutreiben, um rechtsverbindliche Beschlüsse der DSK zu ermöglichen (siehe hierzu auch meinen Tätigkeitsbericht 2020, S. 33 u. 35). BMI zeigte sich diesbezüglich zwar nicht abgeneigt, plant aber auch keine weiteren Schritte mit Verweis darauf, dass hierfür eine Grundgesetzänderung erforderlich sei. Das Thema ist damit allerdings noch nicht erledigt, schließlich hat sich nachfolgend die Ampelkoalition auf Bundesebene in ihrem Koalitionsvertrag dafür ausgesprochen, die DSK zu institutionalisieren und ihr rechtlich, wo möglich, verbindliche Beschlüsse zu ermöglichen.[3]

Tätigkeitsbericht 2020: ttps://t1p.de/2020-tb

2 Siehe KG Berlin, Vorlagebeschluss vom 06.12.2021 – 3 Ws 250/21.
3 Siehe Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP, S. 17.

F. Rechtsprechung von grundsätzlicher Bedeutung

F.1. Gerichtsurteile zum Auskunftsrecht der betroffenen Person

Das Auskunftsrecht nach Artikel 15 der Datenschutz-Grundverordnung (DS-GVO) ist bereits durch verschiedene Gerichtsurteile – teils unterschiedlich – ausgelegt worden. Nun äußerten sich zwei oberste Gerichtshöfe des Bundes zu wesentlichen Fragen dieses Betroffenenrechtes.

Das Recht auf Auskunft der betroffenen Person gegenüber dem für eine Datenverarbeitung Verantwortlichen ist das zentrale Betroffenenrecht in der DS-GVO. Die umfassende Auskunft über die verarbeiteten personenbezogenen Daten ermöglicht der betroffenen Person erst die Kontrolle der Rechtmäßigkeit der Datenverarbeitung. Auslegungsfragen zum Auskunftsrecht sind daher wesentlich für die Durchsetzung der DS-GVO.

Rechtsprechung zum Auskunftsrecht

Die Auslegung des konkreten Inhalts und des Umfangs des Rechts auf Auskunft nach Art. 15 Abs. 1 DS-GVO und des Rechts auf Kopie nach Art. 15 Abs. 3 DS-GVO war bereits Gegenstand mehrerer, meist zivilrechtlicher und arbeitsrechtlicher Gerichtsverfahren in verschiedenen Bundesländern. Die jeweiligen Entscheidungen betrafen unter anderem die Frage, welche Informationen in Verbindung mit einer Person konkret dem Auskunftsrecht unterfallen, ob und ggf. unter welchen Voraussetzungen die Geltendmachung der Rechte aus Art. 15 DS-GVO rechtsmissbräuchlich sein kann, ob die Erfüllung dieser Rechte wegen eines unverhältnismäßigen Aufwandes verweigert werden darf und ob es sich bei dem Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO um ein eigenständiges Recht handelt. Die verschiedenen Gerichte bewerteten diese Fragen teils unterschiedlich, sodass eine gefestigte Rechtsprechung rund um das Auskunftsrecht derzeit kaum angenommen werden kann.

Urteil des Bundesarbeitsgerichts vom 27. April 2021

Auseinandersetzung nach Ende des Arbeitsverhältnisses

Als erstes der höchsten deutschen Gerichte äußerte sich 2021 das Bundesarbeitsgericht (BAG) zum Recht aus Art. 15 DS-GVO (Urteil v. 27. April 2021 – 2 AZR 342/20). In dem Sachverhalt ging es um einen typischen Fall einer datenschutzrechtlichen Auseinandersetzung zwischen Arbeitnehmer und Arbeitgeber nach Beendigung des Arbeitsverhältnisses, nämlich einer Klage auf Auskunft über alle beim ehemaligen Arbeitgeber vorhandenen personenbezogenen Daten sowie auf Herausgabe einer Kopie dieser Daten. Darin eingeschlossen sollte auch der gesamte E-Mail-Verkehr sein, in welchem der Kläger namentlich genannt wurde. Leider ließ das BAG die grundsätzliche Frage offen, ob das Recht auf Kopie auch die Herausgabe sämtlicher zwischen Verantwortlichem und betroffener Person gesendeter E-Mails und Schreiben umfasst. Denn nach Auffassung des Gerichts fehlte es im vorliegenden Klageverfahren an einem hinreichend bestimmten Klagebegehren im Sinne von § 253 Abs. 2 Nr. 2 Zivilprozessordnung (ZPO). Die abstrakte Nennung der Kategorien von E-Mails, von denen eine Kopie überlassen werden soll, z. B. solcher von oder an die dienstliche E-Mail-Adresse sowie solcher, in welchen der Auskunftsbegehrende namentlich erwähnt wird, erfüllt nach Ansicht des BAG nicht die Voraussetzungen eines hinreichend bestimmten Klageantrags. Festzustellen ist nach dem BAG-Urteil jedoch zumindest in arbeitsrechtlichen Streitigkeiten, dass eine genaue Benennung der gewünschten Dokumente erforderlich ist und die unbestimmte Forderung auf Herausgabe des gesamten E-Mail-Verkehrs nicht zulässig ist.

BAG fordert genaue Benennung der gewünschten Dokumente

Meiner Auffassung nach ist diese Auslegung des Rechts auf Kopie nach Art. 15 Abs. 3 DS-GVO jedoch zu restriktiv. Erwägungsgrund 63 stellt zwar fest, dass der Verantwortliche eine Konkretisierung der herauszugebenden Unterlagen durch die betroffene Person verlangen kann. Es steht der betroffenen Person jedoch dennoch frei, eine Herausgabe sämtlicher beim Verantwortlichen vorhandenen personenbezogenen Daten zu verlangen. Dies folgt dem Zweck des Auskunftsrechts aus Art. 15 DS-GVO, die Möglichkeit der umfassenden Kontrolle der Rechtmäßigkeit der Datenverarbeitung durch die betroffene Person selbst. Die betroffene Person hat als Außenstehende regelmäßig keinen Einblick in die konkret vorhandenen Informationen zu ihrer Person. Eine Benennung der konkret gewünschten

Dokumente ist ihr daher in vielen Fällen nicht möglich, sodass das Recht auf Auskunft ins Leere liefe.

Urteil des Bundesgerichtshofs vom 15. Juni 2021

Auch der Bundesgerichtshof (BGH) entschied einen Streitfall zum Recht auf Auskunft nach Art. 15 DS-GVO und stellte im Urteil vom 15. Juni 2021 (VI ZR 576/19) wichtige Grundsätze zur Frage des Umfangs des Rechts auf Auskunft auf. Im entschiedenen Verfahren ging es um den Anspruch eines Versicherungsnehmers gegenüber einer Versicherungsgesellschaft auf Herausgabe einer Kopie des vollständigen Prämienkontos und etwaiger erteilter Zweitschriften und Nachträge zum Versicherungsschein sowie um eine Auskunft bezüglich sämtlicher Telefongespräche und Bewertungsvermerke zum Versicherungsverhältnis.

BGH: Begriff der personenbezogenen Daten weit auslegen

Der BGH stellte mit diesem Urteil höchstrichterlich klar, dass der Begriff der personenbezogenen Daten im Zusammenhang mit dem Auskunftsrecht weit auszulegen sei. Mit Blick auf die Definition in Art. 4 Nr. 1 DS-GVO umfasse der Begriff der personenbezogenen Daten alle Informationen zu einer identifizierten oder identifizierbaren natürlichen Person, wobei ein Bezug zu einer bestimmten oder bestimmbaren Person bereits dann bestehe, wenn die Information aufgrund ihres Inhalts, ihres Zwecks oder ihrer Auswirkungen mit der jeweiligen Person verknüpft seien. Daher umfasst das Recht auf Auskunft nach Art. 15 DS-GVO nach der Entscheidung des BGH auch Dokumente wie die wechselseitige Korrespondenz zwischen betroffener Person und Verantwortlichem einschließlich der gesendeten E-Mails sowie einschließlich interner Gesprächs- und Telefonvermerke und interner Bewertungen mit Bezug zur betroffenen Person. Insbesondere sind nach Auffassung des BGH auch Dokumente, welche die betroffene Person bereits kennt oder welche sich bereits in ihrem Besitz befinden (müssten), nicht vom Recht aus Art. 15 DS-GVO ausgeschlossen, da sich die Auskunft auch gerade darauf beziehe, ob das entsprechende Dokument noch beim Verantwortlichen vorhanden ist.

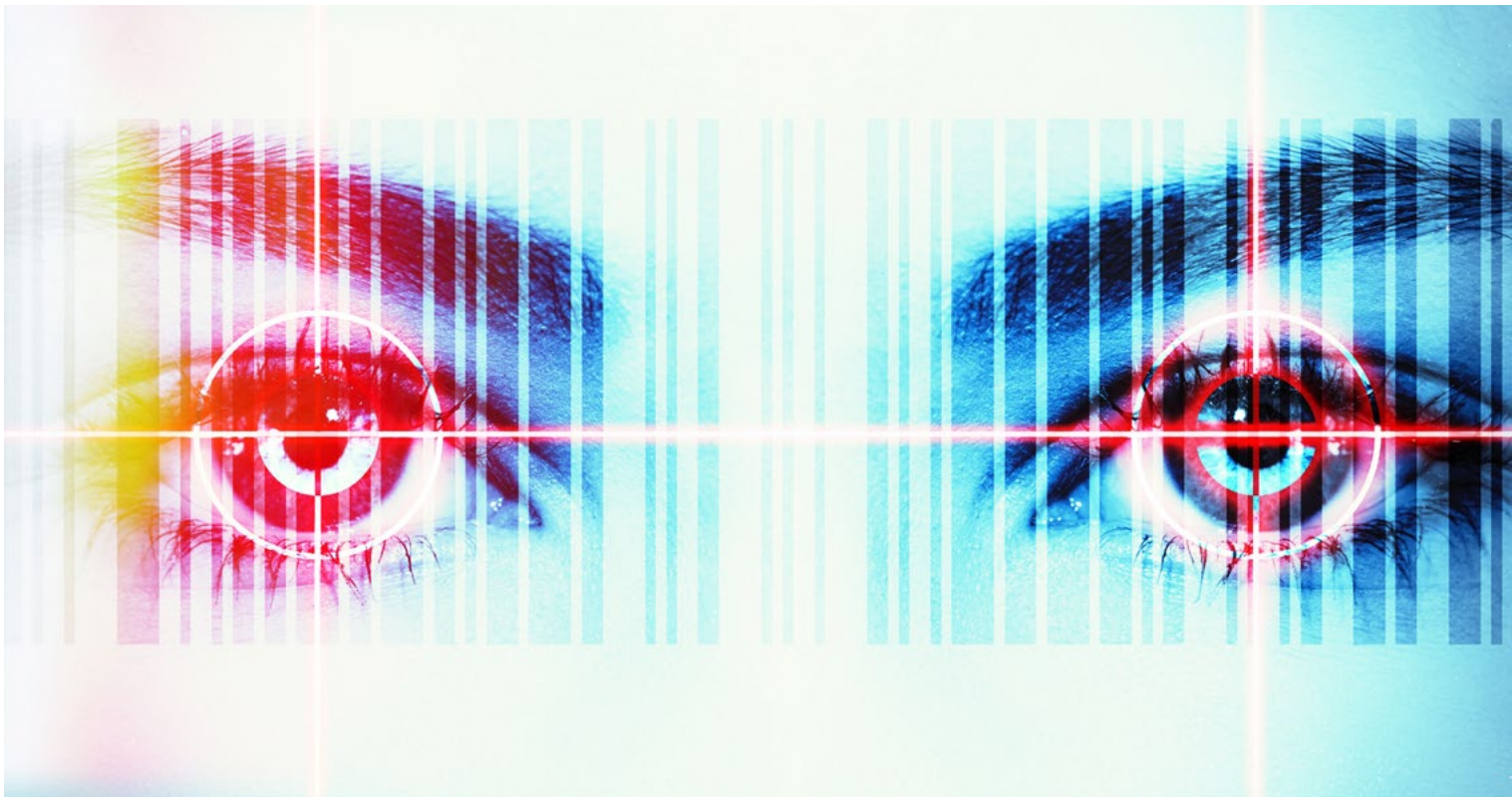
Auch interne Vermerke unterfallen dem Auskunftsrecht

Interne Vermerke sind nach dem BGH Teil der im Rahmen des Auskunftsrechts zu berücksichtigenden Dokumente, da Art. 15 DS-GVO weder seinem Wortlaut noch nach seinem Sinn und Zweck voraussetze, dass es sich um extern zugängliche Daten handelt. Die Entscheidung des BGH ist richtungsweisend in Bezug auf den Umfang der bereitzustellenden Daten: Sämtliche Dokumente mit einem Bezug zu einer bestimmten natürlichen Person fallen in den Anwendungsbereich des Auskunftsrechts nach Art. 15 DS-GVO, unabhängig davon, ob das personenbezogene Datum selbst im Vordergrund des Dokumentes steht oder ob die Dokumente der betroffenen Person bereits bekannt sind oder ihr vorliegen. Der oft vorgebrachten Auffassung, der Anwendungsbereich des Auskunftsrechts müsse nach Sinn und Zweck reduziert werden, um die Pflicht zur Auskunft und zur Herausgabe von Kopien in verhältnismäßigem Rahmen erfüllen zu können, hat der BGH eine deutliche Absage erteilt.

In prozessualer Hinsicht hält der BGH anders als das BAG einen Antrag auf Herausgabe sämtlicher mit der eigenen Person in Verbindung stehender Unterlagen für ausreichend.[1] Sollten die obersten Bundesgerichte ihre Ansichten beibehalten, dürfte perspektivisch eine Entscheidung durch den Gemeinsamen Senat der obersten Gerichtshöfe des Bundes erforderlich werden.

Bedeutung der Urteile

Insbesondere das BGH-Urteil stellt einen wichtigen Beitrag zur Diskussion um die Auslegung des Rechts auf Auskunft und auf dar. Ein Verantwortlicher wird nach dieser Entscheidung gegenüber einem Antrag auf Auskunft nicht mehr den Einwand vorbringen können, das Auskunftsrecht umfasse lediglich die Stammdaten zu einer Person oder signifikante biografische Informationen. Das Urteil steht im Einklang mit der besonderen Bedeutung des Rechts auf Auskunft, der betroffenen Person durch die größtmögliche Transparenz bei der Datenverarbeitung eine gewisse Kontrolle über den Umgang mit den eigenen Daten zurückzugeben.



1 Der BGH hielt einen allgemeinen Auskunftsantrag (Antrag, die Beklagte zu verurteilen, dem Kläger eine vollständige – über den Umfang der Anlagen ... hinausgehende – Datenauskunft durch Überlassen in Kopie – hilfsweise in Textform – zu erteilen) für hinreichend bestimmt im Sinne von § 253 Abs. 2 Nr. 2 ZPO.

F.2. Klage von Betroffenen gegen die Beschwerdeentscheidung der Aufsichtsbehörde

Jede betroffene Person hat gemäß Art. 77 Abs. 1 DS-GVO das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde, wenn sie glaubt, dass eine bestimmte sie betreffende Datenverarbeitung gegen die DS-GVO verstößt. Entsprechen der Umgang der Aufsichtsbehörde mit der Beschwerde und das Ergebnis der Prüfung nicht den Erwartungen der Beschwerde führenden Person, kann es zu einer Auseinandersetzung vor Gericht kommen.

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. Daneben steht jeder natürlichen Person nach Art. 78 Abs. 1 DS-GVO ein Recht auf Klage vor Gericht gegen einen sie betreffenden rechtsverbindlichen Beschluss der Aufsichtsbehörde zu. Die der Beschwerde führenden Person mitgeteilte Entscheidung der Aufsichtsbehörde über das Ergebnis ihrer Beschwerde stellt einen solchen rechtsverbindlichen Beschluss dar.

Möglichkeit der gerichtlichen Überprüfbarkeit

Das Recht auf Beschwerde im Tätigkeitsbericht 2019: https://t1p.de/TB2019

Die Aufsichtsbehörde verfügt über Ermessen, wie und in welchem Umfang sie eine Beschwerde prüft und welche Maßnahmen sie gegebenenfalls gegen eine verantwortliche Stelle anwendet. Dies entscheidet sich gemäß Erwägungsgrund 141 DS-GVO nach der Angemessenheit im Einzelfall.

Von den Gerichten unterschiedlich beantwortet wird die Frage, inwieweit die Entscheidung der Aufsichtsbehörde (wie sie mit einer Beschwerde umgeht, wie sie diese rechtlich bewertet und welche aufsichtsbehördlichen Maßnahmen sie ergreift) gerichtlich überprüfbar ist. Die Auslegung des Inhalts des gerichtlichen Rechtsbehelfs gegen Beschwerdeentscheidungen der Aufsichtsbehörde nach Art. 78 Abs. 1 DS-GVO ist strittig. Teilweise wird das Recht auf Beschwerde bei der Aufsichtsbehörde lediglich als eine Art Petitionsrecht ausgelegt. Dementsprechend bestünde nur ein Anspruch auf Entgegennahme und Befassung mit der Beschwerde und keine weitergehende inhaltliche Überprüfbarkeit durch das angerufene Gericht (OVG Rheinland-Pfalz, Urteil

vom 26. Oktober 2020 – 10 A 10613/20; VG Berlin, Beschluss vom 28. Januar 2019 – VG 1 L 1.19, bestätigt durch OVG Berlin-Brandenburg, Beschluss vom 14. August 2019 – OVG 12 S 30.19/OVG 12 M 29.19).

Nach anderer Ansicht steht der Beschwerde führenden Person zumindest ein Anspruch auf ermessensfehlerfreie Entscheidung der Aufsichtsbehörde über ihre Beschwerde zu, welche auch gerichtlich vollumfänglich überprüfbar ist (VG Hamburg, Urteil vom 27. September 2021 – 17 K 3119/21).

Auffassung des VG Hannover

Das VG Hannover hatte sich mit dieser strittigen Frage auseinanderzusetzen, als ein Beschwerdeführer nach einer Abweisung seiner Beschwerde durch meine Behörde Klage auf aufsichtsbehördliches Einschreiten gegen die verantwortliche Stelle erhob. Der Kläger hatte die Löschung seiner personenbezogenen Daten bei einem Inkassounternehmen verlangt. Meine Behörde hatte jedoch entschieden, dass diesem Löschungsbegehren handels- und steuerrechtliche Aufbewahrungspflichten entgegenstehen und die Beschwerde entsprechend abgewiesen. Das Gericht gab meiner Behörde inhaltlich recht und wies die Klage mit Urteil vom 15. Juli 2021 ab (Az. 10 A 3247/21).

Inhaltliche Prüfmöglichkeit des Gerichts liegt nahe

In Ergänzung zu seiner Entscheidung äußerte sich das VG Hannover in diesem Verfahren ausführlich zum gerichtlichen Rechtsbehelf der betroffenen Person gegen die Aufsichtsbehörde nach Art. 78 Abs. 1 DS-GVO. Nach Auseinandersetzung mit der bestehenden unterschiedlichen Rechtsprechung erklärte das VG Hannover, dass die Annahme einer vollumfänglichen inhaltlichen Prüfmöglichkeit des Gerichts bei einer Klage nach Art. 78 Abs. 1 DS-GVO jedenfalls nahe liege. Denn Erwägungsgrund 141 S. 1 DS-GVO betone das Recht der betroffenen Person auf einen wirksamen gerichtlichen Rechtsbehelf. Hinzu komme das schon in Art. 47 Abs. 1 EU-Grundrechte-Charta festgelegte Gebot des effektiven Rechtsschutzes. Nach Ansicht des VG Hannover setzen ein wirksamer Rechtsbehelf und effektiver Rechtsschutz voraus, dass Entscheidungen der Aufsichtsbehörde im Beschwerdeverfahren auch tatsächlich durch ein Gericht überprüfbar und die Entscheidung des Gerichts im Folgenden durchsetzbar seien. Die Möglichkeit der betroffenen Person, sich mit einer Klage nach Art. 79 DS-GVO direkt gegen eine Datenverarbeitung durch den Verantwortlichen zu wehren, ändert nach Auffassung des VG mangels eines eindeutigen Vorrangverhältnisses der Klagemöglichkeiten hieran nichts.

Diese Auffassung wiederholte das VG Hannover in seinem Urteil vom 18.11.21 (Az. 10 A 5163/21), in welchem wiederum über eine Klage auf aufsichtsbehördliches Einschreiten nach Abweisung einer Beschwerde zu entscheiden war.

Bewertung und Ausblick

Das VG Hannover hat in den beiden geschilderten Urteilen seine Tendenz zur Annahme einer vollumfänglichen gerichtlichen Überprüfbarkeit der Entscheidungen der Aufsichtsbehörde hinsichtlich der ergriffenen Untersuchungsmaßnahmen und der Bewertung des Beschwerdegegenstands

aufgezeigt. In künftigen Verfahren ist daher von einer solchen inhaltlichen Überprüfung durch das Gericht auszugehen. Denkbar sind in der Folge Verurteilungen zu einer erneuten Prüfung und Bescheidung der Beschwerde unter Berücksichtigung der Rechtsauffassung des Gerichts. Die Rechte der Beschwerde führenden Person werden damit gestärkt. Ein Anspruch auf eine bestimmte Maßnahme der Aufsichtsbehörde gegen eine verantwortliche Stelle kann daraus jedoch nicht grundsätzlich abgeleitet werden. Denn die Aufsichtsbehörde verfügt gemäß Art. 58 DS-GVO über ein eigenes Ermessen zur Anwendung der aufsichtsbehördlichen Maßnahmen, welches lediglich bei einer Ermessensreduzierung auf Null eingeschränkt ist.[1]

Rechte der Beschwerde führenden Person gestärkt

Die Frage des genauen Inhalts des Beschwerderechts und der Möglichkeit einer gerichtlichen Überprüfung liegt inzwischen dem Europäischen Gerichtshof zur Vorabentscheidung vor (VG Wiesbaden, Beschluss vom 31.08.21 – 6 K 226/21.WI), so dass mit einer höchstrichterlichen Entscheidung zu rechnen ist.

1 Siehe ausführlich in meinem Tätigkeitsbericht 2020 „Das Recht auf Beschwerde bei der Aufsichtsbehörde", S. 78.

F.3. Entscheidung des Landgerichts Berlin zur Bußgeldverhängung gegen Unternehmen

Haften Unternehmen unmittelbar für Verstöße gegen die DS-GVO durch eine im Unternehmen tätige Person? Diese Frage ist durch die Entscheidung des Landgerichts (LG) Berlin vom 18. Februar 2021 (Az. 526 OWi 1/20) erneut aufgeworfen worden.

Die nach der Datenschutz-Grundverordnung (DS-GVO) in Art. 83 vorgesehene unmittelbare bußgeldrechtliche Haftung einer juristischen Person oder Personenvereinigung für einen im Unternehmen begangenen datenschutzrechtlichen Verstoß ohne weitere Voraussetzungen gerät formal in Konflikt mit den Zurechnungsvorschriften des deutschen Ordnungswidrigkeitenrechts in §§ 30, 130 Ordnungswidrigkeitengesetz (OWiG). Demnach haftet ein Unternehmen nur dann für einen Verstoß, wenn dieser durch eine konkret bestimmte Leitungsperson begangen wurde. Der Umgang mit diesem Rechtskonflikt ist umstritten.

Landgericht Bonn bestätigt Auffassung der Aufsichtsbehörden

Die Datenschutzaufsichtsbehörden vertreten europaweit die Auffassung, dass sich bereits aus der DS-GVO eine unmittelbare Haftung der Unternehmen für Verstöße ergibt. Denn Geldbußen werden nicht gegen einzelne im Unternehmen beschäftigte natürliche Personen verhängt, sondern immer gegen das Unternehmen als Verantwortlichen selbst. Einem Unternehmen wird dabei das Verhalten aller ihr zuordenbaren, natürlichen Personen zugerechnet. Eine nationale Zurechnungsnorm wie § 30 OWiG, welche eine bußgeldrechtliche Haftung des Verantwortlichen durch die Festlegung zusätzlicher Voraussetzungen erschwert, darf aufgrund des europarechtlichen Vorrangs nicht angewendet werden. Dementsprechend hatte das Landgericht Bonn die Nichtanwendbarkeit der Regelungen des deutschen Ordnungswidrigkeitenrechts zur Bußgeldfestsetzung gegen Unternehmen mit Urteil vom 11. November 2020 (Az. 29 OWi 1/20) bestätigt. Eine Darstellung des Rechtsstreits und des Urteils finden Sie auf Seite 86 in meinem Tätigkeitsbericht für das Jahr 2020.

Tätigkeitsbericht 2020: https://t1p.de/2020-tb

Abweichende Auffassung des Landgerichts Berlin

Das LG Berlin entschied mit Beschluss vom 18. Februar 2021, dass sich die Verhängung einer Geldbuße gegen Unternehmen auch im Datenschutzrecht nach den Anforderungen des § 30 OWiG richtet und demnach nur bei Nachweis einer rechtswidrigen Tat durch eine Leitungsperson möglich ist. In dem hier entschiedenen Fall hatte die Berliner Datenschutzaufsichtsbehörde ein Bußgeld gegen ein Unternehmen festgesetzt, das keine Maßnahmen zur regelmäßigen Löschung nicht mehr benötigter oder in sonstiger Weise zu Unrecht gespeicherter personenbezogener Daten getroffen hatte (Verstoß gegen Art. 25 Abs. 1, Art. 5 Abs. 1 Buchstaben a, c und e und Art. 6 Abs. 1 DS-GVO). Das LG Berlin stellte das Verfahren nach Einspruch des Unternehmens wegen eines angenommenen Verfahrenshindernisses ein. Nach Auffassung des LG Berlin ist die Festsetzung eines Bußgeldes gegen ein Unternehmen nur unter den weitergehenden Voraussetzungen des § 30 OWiG zulässig, welche hier im Bußgeldbescheid nicht dargelegt waren. Das LG Berlin vermag eine unmittelbare Haftung von Unternehmen nicht allein aus der DS-GVO selbst herzuleiten, so dass über die Verweisungsnorm des § 41 Bundesdatenschutzgesetz (BDSG) die Regelungen zur Sanktionierung von Unternehmen nach § 30 OWiG anwendbar seien.

Kammergericht legt Fragen dem EuGH vor

Die zuständige Staatsanwaltschaft war mit dieser Entscheidung nicht einverstanden und legte sofortige Beschwerde zur Entscheidung durch das Kammergericht Berlin ein. Mit Beschluss vom 6. Dezember 2021 (Az. 3 Ws 250/21) entschied das Kammergericht, die durch das Verfahren aufgeworfenen Fragen dem Europäischen Gerichtshof (EuGH) zur Vorabentscheidung vorzulegen. Dies betrifft konkret die Fragen, ob Art. 83 DS-GVO dahingehend auszulegen ist, dass ein Bußgeldverfahren unmittelbar gegen ein Unternehmen geführt werden kann, ohne dass es der Feststellung einer durch eine natürliche und identifizierte Person begangenen Tat bedarf bzw. ob das Unternehmen die durch eine beschäftigte Person begangene Tat schuldhaft begangen haben muss.

Bewertung der Entscheidung des LG Berlin

Die Entscheidung des LG Berlin gibt keinen Anlass zur Änderung der von den Aufsichtsbehörden vertretenen Auffassung zur unmittelbaren Unternehmenshaftung. Das LG Berlin verkennt den europarechtlichen Anwendungsvorrang der unmittelbar in den Mitgliedstaaten geltenden DS-GVO mit ihren abschließenden und eindeutigen Regelungen zur Verhängung von Geldbußen gegen Unternehmen als Verantwortliche gegenüber abweichenden nationalen Regelungen. Abgesehen vom eindeutigen Wortlaut der Bußgeldnorm in Art. 83 DS-GVO wird die unmittelbare Unternehmenshaftung auch klargestellt durch Erwägungsgrund 150 der DS-GVO, welcher für die Verhängung von Geldbußen gegen Unternehmen auf die Anwendung des funktionalen Unternehmensbegriffs des europäischen

Unternehmen haften für Fehlverhalten von Beschäftigten

Primärrechts (Art. 101, 102 des Vertrags über die Arbeitsweise der Europäischen Union) verweist. Nach der Rechtsprechung des EuGH zum funktionalen Unternehmensbegriff haften Unternehmen uneingeschränkt für das Fehlverhalten ihrer Beschäftigten.[1] Der EuGH betont weiter das europarechtliche Effektivitätsgebot, demzufolge im nationalen Recht wirksame und hinreichend abschreckende Sanktionen für Verstöße bestehen müssen.[2] Daher darf eine Verhängung von Bußgeldern für Datenschutzverstöße nicht davon abhängig sein, ob es einer Aufsichtsbehörde gelingt, unternehmensinterne Verantwortlichkeiten zu klären. In Unternehmen werden besonders große Mengen an personenbezogenen Daten verarbeitet; gerade hier ist eine wirksame Durchsetzung des Datenschutzrechts von besonderer Bedeutung.

Der Umgang mit personenbezogenen Daten im Unternehmen eröffnet erst die besondere Gefahr eines Verstoßes gegen das Datenschutzrecht, dies begründet die unmittelbare Haftung für jedweden Verstoß. Dem Unternehmen kommt einerseits der Nutzen dieser Datenverarbeitung zugute, daher hat es andererseits auch das Risiko eines Verstoßes innerhalb des Unternehmens zu tragen. Das Unternehmen hat es schließlich selbst in der Hand, durch ein gründliches Datenschutz-Management eine mögliche Haftung zu vermeiden.

Vor diesem Hintergrund erwarte ich, dass sich der EuGH in dieser für die behördliche Praxis wichtigen Frage klar für eine unmittelbare Verbandshaftung von Unternehmen aussprechen wird.

1 EuGH, Urt. v. 07.06.1983, Rs. 100 bis 103/80, Rn. 97
2 EuGH 11.06.2009 – C-429/07 „Inspecteur van de Belastingdienst"

F.4. EuGH-Urteil zur Klagebefugnis der nicht-federführenden Aufsichtsbehörde

Der Europäische Gerichtshof (EuGH) hat mit Grundsatzurteil vom 15. Juni 2021 – Rs. C-645/19 entschieden, dass im Rahmen des One-Stop-Shop-Verfahrens eine Aufsichtsbehörde gemäß Art. 58 Abs. 5 DS-GVO vor dem eigenen nationalen Gericht auch dann wegen vermeintlicher Verstöße gegen die DS-GVO klagen darf, wenn sie nicht die federführende Aufsichtsbehörde ist. Voraussetzung dafür bleibt aber, dass die Vorgaben der Art. 56 ff. DS-GVO eingehalten werden.

Die belgische Datenschutzaufsichtsbehörde hatte bereits vor Inkrafttreten der DS-GVO eine Klage auf Unterlassung der vermeintlich unzulässigen Verarbeitung von personenbezogenen Daten belgischer Internet-Nutzerinnen und -Nutzer durch Cookies oder Social Plugins bei Vorliegen unwirksamer Einwilligungserklärungen gegen Facebook Ireland und Facebook Belgium erhoben. In erster Instanz hatte die Aufsichtsbehörde Erfolg. Das von Facebook angerufene Berufungsgericht äußerte jedoch Zweifel an der Befugnis der belgischen Aufsichtsbehörde zur Erhebung einer eigenen Unterlassungsklage gegen die in Irland ansässige Facebook Ireland Ltd. Das Gericht bezog sich dabei auf die mit der DS-GVO eingeführten Verfahrens- und Zuständigkeitsregelungen bei grenzüberschreitenden Sachverhalten und legte dem EuGH verschiedene Fragen zu den Befugnissen der einzelnen, nicht federführenden Aufsichtsbehörde als Vorabentscheidungsersuchen nach Art. 267 AEUV vor.

Urteil des Gerichtshofs: https://t1p.de/Urteil-Gerichtshof

Der EuGH stellte fest, dass nach der Ausgestaltung des Kooperationsverfahrens in der DS-GVO grundsätzlich die federführende Aufsichtsbehörde für Maßnahmen aufgrund von datenschutzrechtlichen Verstößen zuständig sei. Die Zuständigkeit einer anderen betroffenen Aufsichtsbehörde sei dagegen die Ausnahme (etwa in den Fällen des Art. 56 Abs. 2 und Art. 66 DS-GVO). Die Befugnis einer betroffenen Aufsichtsbehörde zur Geltendmachung eines vermeintlichen Verstoßes vor einem Gericht des eigenen Mitgliedstaates nach Art. 58 Abs. 5 DS-GVO bleibe davon jedoch unberührt, soweit dies im Einklang stehe mit den Regelungen zur Zuständigkeit und den Verfahren der Zusammenarbeit und Kohärenz. Dies könne etwa dann der Fall sein, wenn die federführende Aufsichtsbehörde nach Unterrichtung durch die betroffene Aufsichtsbehörde entscheidet, sich nicht selbst mit dem Fall zu befassen (Art. 56 Abs. 5 in Verbindung mit Art. 61, 62 DS-GVO) oder wenn die betroffene Aufsichtsbehörde eine einstweilige Maßnahme im Hoheitsgebiet ihres Mitgliedstaats nach Art. 61 Abs. 8 DS-GVO ergreift, nachdem die federführen-

de Aufsichtsbehörde nach einem Ersuchen um Amtshilfe nicht die erforderlichen Informationen übermittelt hat (Art. 61 Abs. 1 in Verbindung mit Art. 61 Abs. 8 DS-GVO).

Die Regelung des Art. 58 Abs. 5 DS-GVO entfalte unmittelbare Geltung, sodass eine Aufsichtsbehörde sich auf ihre Befugnis zur Klage gegen Private bei Verstößen gegen die DS-GVO berufen könne, auch wenn die Vorschrift in dem betreffenden Mitgliedstaat nicht besonders umgesetzt worden ist.

Bewertung des Urteils

Ich bewerte dieses Urteil positiv. Zum einen hat der EuGH die Vorgaben der DS-GVO zum Verhältnis von federführender und betroffener Aufsichtsbehörde zueinander präzisiert. Die Maximen der grundsätzlichen Zuständigkeit der federführenden Aufsichtsbehörde und der nur in Ausnahmefällen bestehende Befugnis der betroffenen Aufsichtsbehörde zu eigenen Maßnahmen wurden dabei nicht in Frage gestellt. Zum anderen hat der EuGH klargestellt, dass jede Aufsichtsbehörde die Befugnis zur direkten Klage bei vermeintlichen Verstößen aus Art. 58 Abs. 5 DS-GVO hat und damit die Möglichkeiten der Aufsichtsbehörden zu einem Vorgehen bei Datenschutzverstößen erweitert.

Verhältnis der Aufsichtsbehörden zueinander präzisiert

Die Klarstellung des Gerichtes, dass sich die Aufsichtsbehörden unmittelbar auf Art. 58 Abs. 5 DS-GVO berufen können, auch wenn keine spezifische Umsetzung in der jeweiligen nationalen Rechtsordnung erfolgt ist, begrüße ich. Zwar sehe ich im nicht-öffentlichen Bereich keinen erkennbaren Vorteil darin, Abhilfemaßnahmen nicht per Verwaltungsakt zu verfügen, sondern auf dem Klageweg einzufordern. Allerdings halte ich es nicht für ausgeschlossen, dass im öffentlichen Bereich Bedarf besteht, dass Deutschland Art. 58 Abs. 5 DS-GVO umsetzt und es den Aufsichtsbehörden ermöglicht, gerichtliche Verfahren wegen DS-GVO-Verstößen einzuleiten. Zudem sollte das Urteil zum Anlass genommen werden zu prüfen, ob Aufsichtsbehörden in gerichtlichen Ordnungswidrigkeitenverfahren nicht selbst als Verfahrensbeteiligte die Einleitung eines gerichtlichen Verfahrens betreiben oder sich hieran beteiligen können müssten, ohne dabei von der Verfahrensherrschaft der Staatsanwaltschaft abhängig zu sein.

G. Beteiligung an Gesetzgebungsverfahren

G.1. Übersicht begleiteter Rechtssetzungsvorhaben

Die Begleitung von Rechtssetzungsvorhaben ist ein bedeutender Teil meiner Arbeit und nimmt dementsprechend viel Raum ein. Die folgende Übersicht soll das verdeutlichen, bevor ich anschließend auf einige Verfahren näher eingehe.

Gesetze

- Änderung Nds. Ausführungsgesetz zum SGB VIII (Einführung Ombudstelle)
- Änderung Ausführungsgesetz Transplantationsgesetz
- Nds. Ausführungsgesetz zum Bundesmeldegesetz
- Nds. Abschiebungshaftvollzugsgesetz
- Gesetz zur Änderung des Nds. Ausführungsgesetzes zum Tiergesundheitsgesetz
- Gesetz zur Änderung des Nds. Jagdgesetzes
- Änderung Nds. Bauordnung
- Änderung Nds. Pflegegesetz
- Nds. Ausführungsgesetz zum Zensusgesetz 2022
- Änderung Nds. Glücksspielgesetz
- Änderung Nds. Architektengesetz
- Änderung Nds. Ingenieurgesetz
- Änderung Nds. Spielbankengesetz
- Änderung Nds. Gesetz über Schulen für Gesundheitsfachberufe und Einrichtungen für die praktische Ausbildung (NSchGesG)
- Gesetz über die Beantwortung von Auskunftsverlangen öffentlicher Stellen durch die berufsständischen Versorgungseinrichtungen
- Änderung Nds. Gesetz zur Durchführung der Marktüberwachung von harmonisierten Bauprodukten (NBauPMÜG)

- Änderung Nds. Berufsqualifikationsfeststellungsgesetzes (NBQFG)
- Änderung Gesetz über den Staatsgerichtshof
- Änderung Nds. Kommunalabgabengesetz
- Änderung Nds. Gesetz über Öffentlich bestellte Vermessungsingenieurinnen und Öffentlich bestellte Vermessungsingenieure
- Änderung Nds. Gesetz über das amtliche Vermessungswesen
- Änderung Nds. Ausführungsgesetz zum Wasserverbandsgesetz
- Änderung Nds. Verfassungsschutzgesetz (NVerfSchG)
- Änderung Nds. Sicherheitsüberprüfungsgesetz (Nds. SÜG)
- Änderung Nds. Polizeigesetz (NPOG)+
- Änderung Nds. Justizvollzugsgesetz (NJVollzG)
- Änderung Nds. Beamtengesetz (NBG)
- Änderung Nds. Disziplinargesetz (NDiszG)
- Änderung Nds. Katastrophenschutzgesetz (NKatSG)

Verordnungen

- Änderung AnerkVO SGB XI (Anerkennung von Angeboten zur Unterstützung im Alltag)
- DVO NKiTaG (Kita-Gesetz)
- Änderung ZustVO GuS (Gesundheit und Soziales)
- Änderung Nds. Verordnung über Anforderungen an Schulen für Gesundheitsfachberufe und an Einrichtungen für die praktische Ausbildung (NSchGesVO)
- Änderung Nds. Landeswahlordnung (NLWO) und Nds. Kommunalwahlordnung (NKWO)
- Änderung Nds. Durchführungsverordnung zum Baugesetzbuch (DVO BauGB)
- Verordnung über düngerechtliche Anforderungen zum Schutz der Gewässer vor Verunreinigung durch Nitrat oder Phosphat (NDüngGewNPVO)
- Änderung Nds. Verordnung über Meldepflichten in Bezug auf Nährstoffvergleiche und Düngebedarfe sowie über den gesamtbetrieblichen Düngebedarf (NDüngMeldVO) sowie der Nds Verordnung über die Meldepflichten und die Aufbewahrung von Aufzeichnungen in Bezug auf Wirtschaftsdünger (WDüngMeldPflV Nds.)
- Änderung Nds. Verordnung über die Weiterbildung in Gesundheitsfachberufen (NWeibiVO)
- Verordnung über die Mitwirkung und Beleihung von Kontrollstellen im Ökologischen Landbau (MVO-ÖL)
- Nds. Corona-Absonderungsverordnung

- Verordnung Nds. Justizministerium zur elektronischen Aktenführung bei den Gerichten (Nds. eAktGerVO)
- Änderung Nds. Beihilfeverordnung
- Änderung Verordnung über die Gebühren und Auslagen für Amtshandlungen und Leistungen (Allgemeine Gebührenordnung – AllGO –)
- Verordnung über die Ausbildung und Prüfung für Hygienekontrolleurinnen und Hygienekontrolleure im öffentlichen Gesundheitsdienst (APVO-HygK)
- Änderung Lehrverpflichtungsverordnung (LVVO)
- Änderung Verordnung über die Führung notarieller Akten und Verzeichnisse, der Notarfachprüfungsverordnung, der Notarverzeichnis- und -postfachverordnung, der Rechtsanwaltsverzeichnis- und -postfachverordnung und der Patentanwaltsausbildungs- und -prüfungsverordnung sowie zur Einführung der Patentanwaltsverzeichnisverordnung (NotAktVV)

Erlasse/Richtlinien/Sonstiges

- Richtlinie über die Gewährung von Zuwendungen zur Förderung von Selbsthilfegruppe
- Verwaltungsvorschrift zum Nds Ausführungsgesetz Zensusgesetz 2022
- Förderrichtlinie Vereine in sozialen Brennpunkten
- Nds. Dienstwohnungsverwaltungsvorschriften (NDWVV)
- Gem. RdErl. MWK und MS zum Gesundheitsberuf Hebamme („Zuständige Behörde – Regelung“)
- Verhaltensregeln für Notare (BNotKammer)

Staatsverträge

- Staatsvertrag zwischen der Freien und Hansestadt Hamburg und dem Land Niedersachsen und Änderung des Staatsvertrages zwischen der Freien Hansestadt Bremen und dem Land Niedersachsen im Bereich der beiden EU-Fonds EGFL und ELER sowie nationaler Fördermaßnahmen
- Staatsvertrag zwischen der Freien und Hansestadt Bremen und dem Land Niedersachsen im Bereich des Ökologischen Landbaus

G.2. Änderungsgesetz zum Niedersächsischen Verfassungsschutzgesetz

Am 2. August 2021 ist die novellierte Fassung des Niedersächsischen Verfassungsschutzgesetzes (NVerfSchG) in Kraft getreten. Zuvor hatte meine Behörde vor dem zuständigen Ausschuss des Landtages zum Gesetzentwurf Stellung genommen.

Wie ich in meinem letzten Tätigkeitsbericht dargestellt habe, wurden einige meiner Empfehlungen bereits im Rahmen der ministeriellen Bearbeitung berücksichtigt. Bedauerlicherweise wurden jedoch etliche andere Kritikpunkte nicht im parlamentarischen Verfahren aufgegriffen.

Siehe Tätigkeitsbericht 2019, S. 67 ff.: https://t1p.de/TB2019

„Systemwechsel" mit Lücken

Im Rahmen einer öffentlichen Anhörung im Verfassungsschutzausschuss des Landtages im Februar 2021 machte ich deutlich, dass ursprünglich auf Grundlage des § 2 Nummer 2 Buchstabe c des Niedersächsischen Datenschutzgesetzes (NDSG) die Regelungen der DS-GVO auch für den Verfassungsschutz gelten sollten. Mit dem Gesetzentwurf fand jedoch gewissermaßen ein Systemwechsel statt. Anstelle der DS-GVO soll nun grundsätzlich der Zweite Teil des NDSG, der die JI-Richtlinie umsetzt, zur Anwendung kommen. Dieses ist aufgrund der Sachnähe zur Gefahrenprävention und zur Straftatenverhütung durchaus nachvollziehbar. Allerdings lässt die entsprechende Regelung in § 33b NVerfSchG wesentliche Regelungen des Zweiten Teils des NDSG unberücksichtigt. Insofern ist für den Bereich des Verfassungsschutzes teilweise kein angemessenes datenschutzrechtliches Niveau gewährleistet.

So fehlen etwa die von mir empfohlene Aufnahme von Regelungen zur Datenschutz-Folgenabschätzung. Bei Übernahme der Regelungen könnte bei Datenverarbeitungen, die voraussichtlich ein hohes Risiko für Rechte und Freiheiten der Betroffenen beinhalten, in gesetzlich formalisierter Weise festgestellt werden, ob mit den vorgesehenen Schutzmaßnahmen ein ausreichendes Schutzniveau sichergestellt wird. Auch die Aufnahme einer Regelung zur vorherigen Anhörung meiner Behörde vor Inbetriebnahme neuer Datenverarbeitungssysteme wäre insbesondere mit Blick auf den hierbei im Vordergrund stehenden Beratungs- und Unterstützungsgedanken zweckmäßig gewesen. Dem Verfassungsschutz würde hierdurch – gesetzlich verankert – eine fach-

liche Mitprüfung durch meine Behörde sowie eine Beratung zu zusätzlichen Schutzmaßnahmen (insbesondere technischer Natur) zur Verfügung gestellt.

Daneben wäre unter anderem die von mir geforderte Aufnahme von Regelungen zu Datenpannenmeldungen sowie zur Möglichkeit der vertraulichen Meldung von Verstößen empfehlenswert, um ein angemessenes datenschutzrechtliches Niveau zu gewährleisten.

Hohe Hürden für die Erteilung einer Auskunft

Zudem kritisierte ich unter anderem die geplanten Änderungen des Auskunftsanspruchs in § 30 des Gesetzentwurfs. Vor der Erteilung einer Auskunft wird nunmehr der Hinweis auf einen konkreten Sachverhalt sowie die Darlegung eines besonderen Interesses an der Auskunft durch den Betroffenen verlangt. Zudem sind die Herkunft der Daten und die Empfänger der Übermittlung vom Umfang des Auskunftsanspruchs nicht gedeckt. Hierdurch werden die Betroffenenrechte erheblich beschnitten. Zwar sind Beschränkungen in gewissem Maße grundsätzlich zulässig. Die hier vorgesehene Hürde bei der Antragstellung ist jedoch nicht erforderlich und steht konträr zum europäischen Recht.

Bestandsdatenauskunft verfassungswidrig

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

Schließlich ist besonders schwerwiegend, dass der Gesetzentwurf den Beschluss des Bundesverfassungsgerichts zur Bestandsdatenauskunft außer Acht lässt. Erforderliche Anpassungen des § 20 NVerfSchG bleiben unerledigt. Die Regelungen zur Bestandsdatenauskunft sind damit in ihrer jetzigen Fassung nicht verfassungskonform.

G.3. Änderung des Niedersächsischen Justizvollzugsgesetzes

Der Gesetzentwurf der Landesregierung zur Änderung des Niedersächsischen Justizvollzugsgesetzes (NJVollzG) befindet sich weiterhin im parlamentarischen Verfahren. Meine Behörde hat hierzu im Berichtszeitraum sowohl schriftlich als auch mündlich im Rahmen einer Anhörung gegenüber dem zuständigen Unterausschuss des Landtages Stellung genommen.

Zum bisherigen Verlauf des Gesetzgebungsverfahrens habe ich in meinen Tätigkeitsberichten 2017/2018 und 2019 berichtet. Die Novellierung des NJVollzG ist unter anderem durch die europäische Datenschutzreform bedingt. So müssen die Vorgaben der Richtlinie (EU) 2016/680 (JI-Richtlinie) in den datenschutzrechtlichen Bestimmungen des NJVollzG umgesetzt werden. Hinzu kommen durch den Gesetzgeber geplante Ergänzungen, unter anderem zur Schaffung einer Rechtsgrundlage für den Einsatz auf künstlicher Intelligenz basierender Überwachungssysteme in den Niedersächsischen Justizvollzugsanstalten.

Siehe z. B. Tätigkeitsbericht 2019, S. 66: https://t1p.de/TB2019

Anhörung im Ausschuss

Im Sommer 2021 beteiligte sich meine Behörde an einer öffentlichen Anhörung des Unterausschusses „Justizvollzug und Straffälligenhilfe“ des Ausschusses für Rechts- und Verfassungsfragen im Niedersächsischen Landtag. Die Anhörung bezog sich auf die Drucksache 18/3764, die bereits aus dem Herbst 2019 stammte sowie die zwischenzeitlich hierzu eingebrachten weitreichenden Änderungsvorschläge der Fraktionen der SPD und CDU.

Positiv hervorzuheben ist, dass die JI-Richtlinie mit dem Gesetzentwurf nebst Änderungsanträgen in erheblichem Maße weiter umgesetzt wird. Zudem soll nach der grundsätzlichen Zielrichtung des Gesetzentwurfs – insbesondere der Vorlage 13 – die Handhabe der datenschutzrechtlichen Vorgaben möglichst anwendungsfreundlich gestaltet und vereinfacht werden. Dies soll erreicht werden, indem wesentliche datenschutzrechtliche Vorgaben als eigenständige Regelungen in das Gesetz aufgenommen werden. Insbesondere mit Blick auf die Betroffenenrechte ist dies zu begrüßen.

Einsatz „künstlicher Intelligenz"

Besonders kritisch beurteile ich hingegen die Regelung zum Einsatz optisch-elektronischer Einrichtungen in § 213 des Gesetzentwurfs (Vorlage 13). Diese beinhaltet einen potenziell umfassenden Einsatz „künstlicher Intelligenz". Nach dieser Vorschrift ist der Einsatz technischer Assistenzsysteme – auch in „Hafträumen" – sowohl zur Suizidprävention als auch zur Aufrechterhaltung der Sicherheit und Ordnung in der Anstalt mittels entsprechender Situationserkennung vorgesehen. Angesichts dieser weiten Ausgestaltung des Anwendungsbereiches sind umfassende Anpassungen notwendig. Zur Einhaltung des Grundsatzes der Verhältnismäßigkeit müsste die derzeit mit der „Aufrechterhaltung der Sicherheit und Ordnung" sehr weit gefasste Zweckbestimmung auf die Suizidprävention beschränkt werden. Zudem bedarf es einer deutlichen Einschränkung des räumlichen Anwendungsbereichs ausschließlich auf besonders gesicherte Hafträume, in denen die oder der Gefangene insbesondere bei einer Suizidgefahr untergebracht werden darf.

Eine abschließende Bewertung des Gesetzesvorhabens war aufgrund des bis zum Ende des Berichtszeitraums noch laufenden parlamentarischen Verfahrens nicht möglich.

G.4. Änderung des Niedersächsischen Kommunalabgabengesetzes

Das Niedersächsische Kommunalabgabengesetz (NKAG) befindet sich derzeit in der Novellierung. Bereits im Juli 2021 bezog meine Behörde zu dem Referentenentwurf des Gesetzes Stellung. Der überwiegende Teil meiner Anregungen wurde vom Niedersächsischen Ministerium für Inneres und Sport aufgegriffen.

Die vorgesehenen Änderungen des NKAG sind unter anderem erforderlich, um im Bereich der kommunalen Abgaben und Steuern eine ausreichende Rechtsgrundlage für die Datenverarbeitungen zu schaffen. Dies soll durch Verweise auf die entsprechenden Regelungen der Abgabenordnung erreicht werden.

Beteiligung meiner Behörde

Das Innenministerium gab mir frühzeitig Gelegenheit, zum Referentenentwurf des NKAG beratend tätig zu werden. Zudem wurde mir gegenüber im weiteren Verlauf des Gesetzgebungsverfahren nachvollziehbar begründet, warum nicht alle meiner Anpassungsvorschläge vom Fachressort berücksichtigt worden sind. Dies ist im vorliegenden Fall letztendlich divergierender Rechtsauffassungen im Zusammenhang mit der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) im Niedersächsischen Datenschutzgesetz (NDSG) geschuldet.

Ich beabsichtige, die noch offenen Punkte nach Ende des Berichtszeitraums gegenüber dem MI im Zusammenhang mit dem vorgelegten Gesetzentwurf zur Änderung des Niedersächsischen Datenschutzgesetzes und weiterer Gesetze in der Stellungnahme zu Artikel 5 dieses Gesetzentwurfs (Änderung des NKAG) erneut aufzugreifen. In diesem Zusammenhang weise ich auf meine Stellungnahme zu erforderlichen Änderungen des NDSG gegenüber dem Niedersächsischen Landtag vom 23. April 2018 sowie auf die Stellungnahme des Gesetzgebungs- und Beratungsdienstes des Niedersächsischen Landtages vom 4. Mai 2018 hin (siehe Vorlage 4 zur Landtags-Drucksache 18/548 beziehungsweise Vorlage 2 zur Landtags-Drucksache 18/352 sowie Vorlage 16 zur Landtags-Drucksache 18/548).

Insgesamt hat sich die Zusammenarbeit mit dem Innenministerium in diesem Verfahren als konstruktiv erwiesen.

G.5. Gesetz über die Landesbeauftragte oder den Landesbeauftragten für Opferschutz

Seit November 2019 gibt es in Niedersachsen als zentrale Anlaufstelle für die Opfer von Straftaten und ihnen nahestehenden Personen den Landesbeauftragten für Opferschutz (LfO). Für die Datenverarbeitungen dieser noch relativ neuen Stelle ist eine Rechtsgrundlage erforderlich, weshalb sich der LfO Anfang 2021 an meine Behörde mit der Bitte um Beratung wandte.

Der LfO soll unter anderem bei sogenannten Großschadensereignissen von der Polizei die erforderlichen Daten – wie zur Anzahl und Identität von Opfern und sonstigen Betroffenen sowie zur Lage – erhalten, um proaktiv auf Betroffene zugehen zu können. Mit einer derartigen Datenverarbeitung ist eine Zweckänderung verbunden, die besonders gesetzlich zu verankern ist. Für die Erstellung näherer datenschutzrechtlicher Bestimmungen wurde die Form eines eigenen Regelungswerkes gewählt.

Konstruktive Beratungen

Im Sommer 2021 fand ein erstes und sehr konstruktives Beratungsgespräch mit Vertretern des LfO und des Niedersächsischen Justizministeriums (MJ) zum ersten Referentenentwurf des Gesetzes über die Landesbeauftragte oder den Landesbeauftragten für Opferschutz (NLfOG) statt. Der anschließend erstellte überarbeitete Entwurf des NLfOG berücksichtigte bereits etliche meiner Hinweise. Nach nochmaliger Prüfung des aktualisierten Referentenentwurfs beriet meine Behörde im Herbst 2021 erneut zu den noch offenen Punkten. Die Beratung bezog sich dabei unter anderem auf die Regelung von Zweckänderungsbefugnissen, die Ausgestaltung der datenschutzrechtlichen Verantwortlichkeit sowie die Informationspflichten. Die weitere Durchführung des (parlamentarischen) Gesetzgebungsverfahrens stand zum Ende des Berichtszeitraums noch aus.

Als Zwischenergebnis möchte ich die sehr frühe Beteiligung meiner Behörde als ein positives Beispiel für einen konstruktiven Gesetzgebungsprozess festhalten.

G.6. Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes

Der Gesetzentwurf der Landesregierung zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) befindet sich im parlamentarischen Verfahren. Meine Behörde hat hierzu zuletzt im Rahmen einer öffentlichen Anhörung gegenüber dem zuständigen Ausschuss des Landtages Stellung bezogen.

Siehe Tätigkeitsbericht 2019, S. 60: https://t1p.de/TB2019

Zu der vorangegangenen Änderung, die Ende 2019 in Kraft getreten ist, habe ich bereits im Tätigkeitsbericht 2019 ausführlich berichtet. Positiv hervorzuheben ist, dass mit dem aktuellen Gesetzentwurf die bisher nur unzureichende Umsetzung der JI-Richtlinie im allgemeinen Gefahrenabwehrrecht weitgehend abgeschlossen ist. Ein wesentliches Defizit besteht jedoch weiterhin bei der Umsetzung der weitergehenden (Abhilfe-)Befugnisse meiner Behörde, die Artikel 47 JI-Richtlinie zwingend vorschreibt. Hierdurch ist eine effektive datenschutzrechtliche Aufsicht nur unzureichend möglich.

Anhörung im Ausschuss

Der Ausschuss des Landtags für Inneres und Sport gab mir im Rahmen einer öffentlichen Anhörung am 11. Februar 2021 die Möglichkeit zur Stellungnahme. Dabei brachte ich neben der oben erwähnten unvollständigen Umsetzung meiner Aufsichtsbefugnisse als grundlegenden Kritikpunkt an, dass der Gesetzentwurf in seiner derzeitigen Form wenig anwenderfreundlich und praxistauglich gestaltet ist. Ursache hierfür ist ein Regelungsdickicht mit zahlreichen Quer-, Weiter- und Rückverweisungen im NPOG auf andere Rechtsnormen im ersten und zweiten Teil des NDSG sowie in der DS-GVO. Hierdurch dürfte ein enormer Schulungsbedarf und -aufwand für die betroffenen Polizei- und Verwaltungsbehörden entstehen. Dem könnte mittels abschließender datenschutzrechtlicher Regelungen im NPOG oder NDSG abgeholfen werden.

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

Daneben brachte ich an, dass es in § 33 c NPOG an einer (vollständigen) Einhaltung der Vorgaben des Beschlusses des Bundesverfassungsgerichts (BVerfG) zur Bestandsdatenauskunft (siehe auch J.2.6, S. 119) fehlt. Zwar ist nach dem Beschluss die Erteilung einer Auskunft über diese Daten grundsätzlich verfassungsrechtlich zulässig. Unter anderem muss jedoch nach dem „Doppeltürmodell" des BVerfG bei einem Datenaustausch zur staatlichen Aufgabenwahrnehmung sowohl für die Übermittlung der Daten durch die Telekommunikationsanbieter als auch für den Abruf der Daten durch die jeweilige Behörde jeweils eine Rechtsgrundlage geschaffen werden. Diese müssen dem Verhältnismäßigkeitsgebot genügen. Diesen Vorgaben genügt die Regelung des § 33 c NPOG in ihrer derzeitigen Fassung nicht vollumfänglich.

Positiv zu bewerten waren unter anderem eingeführte Regelungen zu Benachrichtigungs- und Dokumentationspflichten sowie die Schaffung einer Rechtsgrundlage für den Einsatz von sogenannten stillen SMS sowie für Datenübermittlungen zur Zuverlässigkeitsprüfung.

Eine abschließende Bewertung war aufgrund des noch laufenden parlamentarischen Verfahrens nicht möglich.

G.7. Änderung des Niedersächsischen Sicherheitsüberprüfungsgesetzes

Das Niedersächsische Sicherheitsüberprüfungsgesetz (SÜG) befindet sich derzeit in der Überarbeitung. Etliche meiner Anpassungsvorschläge zum Referentenentwurf sollen dabei aufgegriffen werden.

Anfang 2021 erhielt meine Behörde vom Niedersächsischen Innenministerium (MI) frühzeitig die Gelegenheit, zum Referentenentwurf zur Änderung des SÜG beratend tätig zu werden. Eine anschließende Stellungnahme des MI zeigte, dass meine Änderungsvorschläge an verschiedenen Stellen berücksichtigt werden sollten: etwa hinsichtlich der näheren Ausgestaltung der Bestimmungen zu Verschlusssachen, Betroffenenrechten, Sicherheitserklärungen und Protokollierungen. Ich empfahl dem Ministerium daraufhin, auch das Auskunftsrecht präziser zu gestalten. So wurde angeregt, grundsätzlich auch Angaben zur Herkunft der Daten mit aufzunehmen. Auch die Hinweispflicht auf die Rechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung sollte ergänzt werden. Denn auf die Betroffenenrechte ist vom Verantwortlichen verpflichtend hinzuweisen. Gleiches gilt für den Hinweis auf das Beschwerderecht bei meiner Behörde. Weiter forderte ich die derzeit in § 21 Absatz 4 des Entwurfs vorgesehene Einschränkung der Auskunft an meine Behörde im Gleichklang zu der entsprechenden Regelung des Niedersächsischen Verfassungsschutzgesetzes zu streichen.

Insgesamt hat sich die Zusammenarbeit mit dem MI hinsichtlich der Änderung des SÜG als sehr konstruktiv erwiesen. Im Rahmen einer sich anschließenden Verbandsbeteiligung würde ich noch einmal eine Möglichkeit zur Stellungnahme zu den zwischenzeitlichen Änderungen am Gesetzentwurf erhalten.

G.8. Datenschützer unterstützen bei der Verwaltungsmodernisierung

Auf der Grundlage des im Frühjahr 2021 in Kraft getretenen Registermodernisierungsgesetzes (RegModG) sollen Verwaltungsleistungen des Staates digitalisiert und vereinfacht werden, so die Hoffnung des Gesetzgebers. Gleichzeitig wird auf Basis der bereits bestehenden Steueridentifikationsnummer eine Bürger-ID geschaffen, die ein neues, mächtiges Identifikationsmerkmal darstellt. Eindringlich hat die Datenschutzkonferenz bereits auf die Gefahren für die Persönlichkeitsrechte von Bürgerinnen und Bürgern hingewiesen, die mit einer solchen Personenkennziffer einhergehen können. Eine enge Begleitung der Umsetzung der Registermodernisierung durch die Datenschutzaufsichtsbehörden ist daher dringend geboten.

Zielbild: https://t1p.de/regmod

Bereits vor der Gesetzesverkündung beschloss der nationale IT-Planungsrat das vom Koordinierungsprojekt Registermodernisierung erarbeitete Zielbild der Registermodernisierung. Zur Umsetzung des Zielbildes rief der nationale IT-Planungsrat in der 35. Sitzung am 23. Juni 2021 das Projekt „Gesamtsteuerung Registermodernisierung“ ins Leben.

Kompetenzteam Recht/Datenschutz

Den Kern der Projektstruktur bildet die Bund-Länder-Transformationseinheit, die die Programmsteuerung wahrnimmt. Als Gremium für übergreifende Programmentscheidungen wurde zudem der Lenkungskreis Registermodernisierung aufgebaut. Eines der vier Kompetenzteams, die das Gesamtprojekt beraten, ist das Kompetenzteam Recht/Datenschutz.

Es ist mir ein besonderes Anliegen, die weiteren Umsetzungsschritte der Registermodernisierung kritisch zu begleiten. Beschäftigte meiner Behörde vertreten die Datenschutzkonferenz und sind sowohl im Lenkungskreis als auch im Kompetenzteam Recht/Datenschutz beratend tätig.

Once-Only-Prinzip zum Nutzen der Bürgerinnen und Bürger

Das Zielbild der Registermodernisierung umfasst zum einen ein Nutzenversprechen an die Bürgerinnen und Bürger. Dazu gehört z. B. die Umsetzung des Once-Only-Prinzips: Künftig sollen Bürgerinnen und Bürger Nachweise für Verwaltungsvorgänge (z. B. die Geburtsurkunde) nur einmal an eine Verwaltungsstelle übermitteln müssen. Anschließend steht der eingereichte Nachweis allen Verwaltungseinheiten zur Verfügung. Bei Nutzung und Austausch derartiger Datensätze sollen hohe Datenschutzstandards bei bestmöglicher Transparenz gegenüber den Bürgerinnen und Bürgern gelten.

Das Zielbild beschreibt vier wesentliche Elemente einer modernisierten Registerlandschaft:

1. Eine interoperable und sichere technische Architektur,
2. anschlussfähige Register auf Seiten der registerführenden Stellen und
3. rechtliche Rahmenbedingungen für einen sicheren und datenschutzkonformen Datenaustausch einschließlich bedarfsgerechter Zugangsmöglichkeiten für die Wissenschaft.

Das Projekt „Gesamtsteuerung Registermodernisierung" unterstützt und steuert die vielen Teilprojekte, die bei der Modernisierung einer vielfältigen Registerlandschaft entstehen. Beispiele für solche Teilprojekte sind die Errichtung einer interoperablen und sicheren Registerinfrastruktur sowie eines Datencockpits, mit dem sich die Bürgerinnen und Bürger Auskünfte über Datenübermittlungen zwischen den öffentlichen Stellen anzeigen lassen können.

Die Registermodernisierung soll in mehreren Schritten über einen Zeitraum von fünf Jahren umgesetzt werden. Phase 1 sollte bis Ende des Jahres 2021 abgeschlossen sein. Im Jahr 2025 soll der laufende Betrieb mit ausgewählten Verwaltungsaufgaben priorisierter Register starten. Ich werde daher dieses wichtige Großprojekt auch in kommenden Jahren beratend und kritisch begleiten.

H. Aufklärung und Öffentlichkeitsarbeit

H.1. Vorträge der Landesdatenschutzbeauftragten

Abgesehen von einer kurzen Phase im Sommer war meine Vortagstätigkeit auch 2021 von Online- und Hybrid-Veranstaltungen geprägt. Bedauerlicherweise machte es die Corona-Pandemie meist unmöglich, in den direkten Kontakt mit anderen Fachleuten, Zuhörerinnen und Zuhörern zu kommen. Nichtsdestotrotz konnte ich im Rahmen von rund 35 Veranstaltungen Vorträge halten und mich an Diskussionsrunden beteiligen.

Diskussionen zu Chancen und Risiken der Digitalisierung

Ein übergeordnetes Thema, das 2021 in vielen verschiedenen Facetten auf der Agenda stand, war wenig überraschend die Digitalisierung. Sei es die Sorge vor dem gläsernen Landwirt, Beschäftigtendatenschutz in Zeiten von Big Data oder das Potenzial von Smart Home Anwendungen zur Gesundheitsprävention – fast jeder Lebensbereich und Wirtschaftszweig muss sich mit den Chancen, aber eben auch den Risiken der Digitalisierung auseinandersetzen. Ich werde dabei nicht müde zu betonen, dass Datenschutz eine wesentliche Voraussetzung für das Gelingen einer Digitalisierung ist, die die Interessen aller Beteiligter berücksichtigt.

Interesse an Vollzugspraxis und Rolle der LfD

Ebenfalls auf großes Interesse stießen im vergangenen Jahre Vorträge zu meiner Vollzugstätigkeit, insbesondere zur Bußgeldpraxis, sowie zu meiner Rolle im Allgemeinen. Das Spektrum der Veranstaltungen reichte dabei von einem Vortrag für regionale Unternehmen aus dem Raum Wolfenbüttel über das Göttinger Forum IT-Recht bis zu einem Online-Kongress der Deutschen Management Akademie Niedersachsen für russische Verwaltungsfachleute.

Darüber hinaus traten 2021 einige aktuelle Themen in den Vordergrund, die sich für Information, Sensibilisierung und fachlichen Austausch anboten. Zum einen waren das die Fragen rund um den internationalen Datenverkehr, die Verantwortliche in Folge des Schrems II-Urteils des Europäischen Gerichtshofs weiterhin vor große Herausforderungen stellen (siehe auch D.1, S. 25). Zum anderen waren Veranstalter sehr am Thema des Nutzer-Trackings interessiert und in diesem Zusammenhang zum Jahresende vor allem am neuen Telekommunikation-Telemedien-Datenschutz-Gesetz (siehe dazu auch J.8.1, S. 162). Beide Themen werden mich und die Datenschutz-Community im Allgemeinen auch in diesem Jahr weiter begleiten.

Internationaler Datenverkehr und Nutzer-Tracking

DS-GVO und europäische Zusammenarbeit

Ein dritter Schwerpunkt meiner Vortragstätigkeit lag auf der Wirksamkeit der Datenschutz-Grundverordnung (DS-GVO) und dabei besonders auf der Zusammenarbeit der europäischen Aufsichtsbehörden, die viele Ressourcen meines Hauses bindet (siehe dazu auch C. ab S. 14).

Das Jahr 2022 hat zu meinem großen Bedauern erneut mit Online-Veranstaltungen begonnen. Doch ich habe Hoffnung, dass im Sommer wieder verstärkt ein direkter Austausch möglich sein wird. Dieser ist in meinen Augen trotz aller technischer Möglichkeiten von Videokonferenzen nach wie vor die effektivere und angenehmere Art, um miteinander ins Gespräch zu kommen.

H.2. Veröffentlichung von Informationsmaterial

Auch im vergangenen Berichtszeitraum habe ich neue Informationsmaterialen zu verschiedenen Bereichen des Datenschutzes veröffentlicht. Die Themen gehen dabei zum Teil auf aktuelle Ereignisse, zum Teil auch auf konkrete Anregungen von außen zurück.

Handreichung zum Download: https://t1p.de/kommunale-abgeordnete

Ein aktuelles Ereignis, das zu einer neuen Publikation führte, war die Kommunalwahl in Niedersachsen. Ratsmitglieder haben in Ausübung ihrer Tätigkeit Zugang zu vertraulichen Daten, die nicht für die Öffentlichkeit bestimmt sind. Gleichzeitig stehen die Mandatsträgerinnen und Mandatsträger vor der Herausforderung, dem Informationsinteresse der Bürgerinnen und Bürger an der Gremienarbeit gerecht zu werden. Um sie dabei zu unterstützen, diesen Balanceakt zu meistern, veröffentlichte ich eine Handreichung zum Datenschutz für kommunale Abgeordnete.

Diese enthält eine Vielzahl von Fallbeispielen aus der täglichen Praxis der Gremienarbeit und weist auf datenschutzrechtliche Fallstricke hin. Einen Schwerpunkt stellt der Umgang mit personenbezogenen Daten von Bürgerinnen und Bürgern in Sitzungsunterlagen und Protokollen dar. Gleichzeitig beantwortet die Handreichung auch Fragen zum Schutz der eigenen Daten der Ratsmitglieder.

Antworten auf Fragen aus der Verwaltung

Alle FAQ im Überblick: https://t1p.de/faq-ueberblick

Ebenfalls für den kommunalen Bereich veröffentlichte ich im Berichtsjahr eine FAQ mit Antworten auf häufig gestellte Fragen zum Datenschutz im Alltag der Verwaltung. Die niedersächsischen Kommunen erbringen als lokale Verwaltungseinheiten vor Ort eine Vielzahl von Leistungen für die Bürgerinnen und Bürger, was mit der Verarbeitung unterschiedlichster personenbezogener Daten einhergeht. Dabei stellen sich häufig Fragen, die einen datenschutzrechtlichen Bezug aufweisen.

Die FAQ greifen vorwiegend allgemeine datenschutzrechtliche Fragestellungen auf und erläutern wichtige Fachbegriffe. Da die Arbeit der Kommunen von der Anwendung einer Vielzahl unterschiedlicher Rechtsgebiete geprägt ist, enthalten die FAQ darüber hinaus auch eine Auflistung der einschlägigen Rechtsgrundlagen, auf die die Kommunen die Verarbeitung personenbezogener Daten stützen können.

Wann ist eine DSFA nötig?

Durch einen Impuls aus der niedersächsischen Wirtschaft entwarf ich ein Prüfschema zur Notwendigkeit einer Datenschutz-Folgenabschätzung (DSFA). Eine DSFA ist eine strukturierte Risikobeurteilung zur Vorab-Bewertung der möglichen Folgen von Datenverarbeitungen. Sie ist dann nötig, wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.

Prüfschema zur DSFA:
https://t1p.de/dsfa-schema

Immer wieder erreichen mich Anfragen dazu, wann eine DSFA konkret durchzuführen ist. Um Anwendern die Beantwortung dieser Frage zu erleichtern, habe ich ein ausführliches, aber gleichzeitig übersichtliches Prüfschema entwickelt. Damit können Datenverarbeiter für ihren Verantwortungsbereich prüfen, ob die Durchführung einer DSFA erforderlich ist. Neben einer Checkliste und einem umfangreichen Glossar der wichtigsten Begriffe enthält das Schema auch Hinweise auf weitere Hilfestellungen zum Thema Datenschutz-Folgenabschätzung.

Weitere Informationsangebote, die sich vornehmlich an die Wirtschaft richten, waren im Berichtszeitraum FAQ zum neuen Telekommunikation-Telemedien-Datenschutz-Gesetz (siehe auch J.8.1, S. 162) sowie eine aktualisierte FAQ für Betriebsräte.

Im Bildungsbereich möchte ich vor allem auf die FAQ zum Einsatz von Videokonferenzsystemen in Schulen (siehe im Detail J.5.2, S. 138) und auf die Eckpunkte zur datenschutzkonformen Durchführung von Online-Prüfungen an Hochschulen (siehe J.5.4, S. 141) hinweisen.

H.3. Online-Schulungen im Datenschutzinstitut Niedersachsen

Da die Corona-Pandemie auch 2021 eine Wiederaufnahme von Fortbildungen in Präsenz unmöglich machte, bot ich im Datenschutzinstitut Niedersachsen (DsIN) Online-Schulungen an. Mit der Resonanz auf dieses neue Angebot war ich sehr zufrieden.

Datenschutzinstitut Niedersachsen: https://t1p.de/dsin-lfd

Zunächst galt es, eine geeignete Plattform zur datenschutzkonformen Durchführung von Schulungen zu finden. Eine wichtige Voraussetzung war hier unter anderem, dass die vor, während und nach der Schulung verarbeiteten personenbezogenen Daten nicht die Europäische Union verlassen und somit durchgehend unter dem Schutz der Datenschutz-Grundverordnung (DS-GVO) stehen. Nachdem dies gelungen war, konnte ich Mitte des Jahres mit den ersten Fortbildungen beginnen.

Neben einer Schulung zu den Grundlagen des Datenschutzes im öffentlichen Bereich bot ich Fortbildungen zum technisch-organisatorischen Datenschutz, zum Datenschutz in der Schule sowie zur datenschutzkonformen Gestaltung von Webseiten an. Sowohl die Themen als auch die Art der Umsetzung wurden gut von den Teilnehmenden angenommen, sodass ich auch 2022 wieder Online-Seminare anbieten werde. Diese werden auch dann Teil meines Fortbildungsangebots bleiben, wenn Präsenzveranstaltungen wieder möglich sind, da sie gerade in einem Flächenland wie Niedersachsen Reisezeit sparen und so mehr Interessierten die Teilnahme ermöglichen.

Denn Präsenzbetrieb wird das DsIN wieder aufnehmen, sobald es die pandemische Lage zulässt. Dies ist umso wichtiger, da sich manche Seminarinhalte nur sehr schwierig auf Distanz vermitteln lassen.

H.4. Kooperation mit der Digitalagentur zur Unterstützung niedersächsischer Unternehmen

Datenschutz ist nicht der Hemmschuh für die Digitalisierung, sondern eine Voraussetzung für deren Gelingen. In diesem Sinne ist die Digitalagentur Niedersachsen eine wichtige Informationsdrehscheibe, um Wirtschaft und Verwaltung für den Wert des Datenschutzes in der Digitalisierung zu sensibilisieren. Die Digitalagentur ist ein Teil der Innovationszentrum Niedersachsen GmbH und vermittelt Beratungs- und Unterstützungsangebote für die niedersächsische Wirtschaft.

Gerade in den durch Digitalisierung geprägten Wirtschaftsbereichen fallen immer mehr Daten an. Sei es bei der Bearbeitung von Kundenaufträgen, im Online-Marketing oder bei Einkäufen im Internet. Diese Daten müssen geschützt werden, die verantwortlichen Stellen tragen eine entsprechend große Verantwortung. Maßgebend für die rechtlich einwandfreie Verarbeitung der Daten sind dabei die Anforderungen der Datenschutz-Grundverordnung (DS-GVO).

Prozess zur Auswahl geeigneter Sicherungsmaßnahmen

Um die niedersächsische Wirtschaft an dieser Stelle wirksam zu unterstützen, engagieren sich meine Mitarbeiterinnen und Mitarbeiter in verschiedenen Formaten der Öffentlichkeitsarbeit der Digitalagentur. So wurde beispielsweise die in meinem Hause entwickelte Methode „ZAWAS“ vorgestellt, welche verantwortliche Stellen bei Auswahl und Aufrechterhaltung geeigneter Sicherungsmaßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten unterstützt. Die Technikneutralität der DS-GVO stellt Verantwortliche bei der technischen Umsetzung der rechtlichen Anforderungen immer wieder vor große Herausforderungen. „ZAWAS“ dient als strukturierte Orientierungshilfe und besteht aus acht logisch aufeinanderfolgenden Schritten, mit denen die angemessenen technischen und organisatorischen Maßnahmen ermittelt werden können.

Potenziale von Open Source Software

Studie im Auftrag des BMI: https://t1p.de/abhaengig

Des Weiteren ging es in einer Diskussionsveranstaltung des Arbeitskreises „IT Sicherheit“ der Digitalagentur um Aspekte der „Sicherheit von Open Source Software“. Die Möglichkeiten des Einsatzes von Open Source Software

ist eine aus Datenschutzsicht hochinteressante Fragestellung. Gerade im Hinblick auf die vieldiskutierte Problematik der beherrschenden Marktposition einiger weniger, großer Anbieter ist die Suche nach Alternativen so aktuell wie nie zuvor. Die Beschaffungs- und Entwicklungsstrategien der Bedarfsträger haben über viele Jahre hinweg tiefe Abhängigkeiten entstehen lassen, wie Studien eindrucksvoll belegen. Die Cloud-Strategien der großen kommerziellen Software-Hersteller bergen an sich schon erhebliche datenschutzrechtliche Risiken im Betrieb, umso mehr jedoch, wenn Datenhaltung oder -verarbeitung in der Cloud in den Anwendungsbereich der problematischen US-Aufklärungsprogramme fallen. Open-Source-Software gewinnt zunehmend eine größere Bedeutung für Unternehmen und Verwaltungen, da insbesondere Fragen der digitalen Souveränität in Deutschland und Europa damit in Verbindung gebracht werden.

Wechsel zu alternativen Produkten wird erleichtert

Ein Vorteil, der vielfach mit quelloffenen Programmen assoziiert wird, ist die höhere Transparenz und die Beachtung offener Standards und Schnittstellen. Deren konsequente Nutzung führt zu einer größeren Produktunabhängigkeit, verbunden mit der Möglichkeit, leichter auf ein alternatives Produkt wechseln zu können. Daher empfehle ich, bei der Beschaffung von Software-Produkten die Möglichkeiten des Einsatzes von Open Source Software stets mit zu prüfen, um zu verhindern, die Abhängigkeit von hochintegrierten, proprietären Paketlösungen immer weiter zu vertiefen. Ferner sollte eine Auftragsverarbeitung ausschließlich im Geltungsbereich der DS-GVO stattfinden, um die rechtlichen Unsicherheiten, die mit einem Drittstaatentransfer von Daten verknüpft sein können, zu vermeiden.

Die Beteiligung an Veranstaltungen der Digitalagentur Niedersachsen stellt sich als wertvolle Ergänzung der Öffentlichkeitsarbeit meines Hauses dar. Gerade die frühzeitige Berücksichtigung datenschutzrechtlicher Anforderungen in die digitalen Innovationsprozesse sind eine wichtige Voraussetzung dafür, dass am Ende nicht nur rechtskonforme Lösungen entstehen. Mindestens ebenso wichtig ist es, durch Vertrauen und Sicherheit im Umgang mit den anvertrauten Daten für deren Akzeptanz und Nachhaltigkeit zu sorgen.

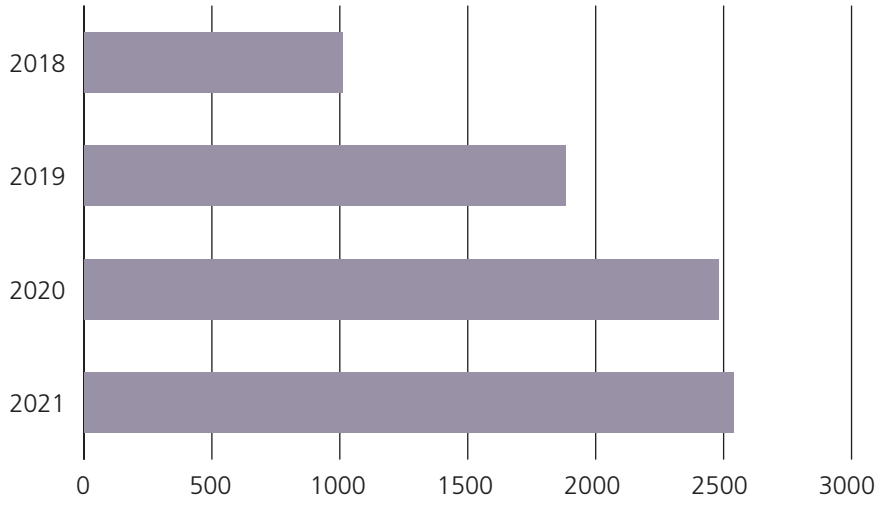
I. Aufsicht und Vollzug

I.1. Zahlen und Fakten

Um einen schnellen Überblick über die Arbeit meiner Behörde zu ermöglichen, veröffentliche ich auch in diesem Jahr 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.

Beschwerden

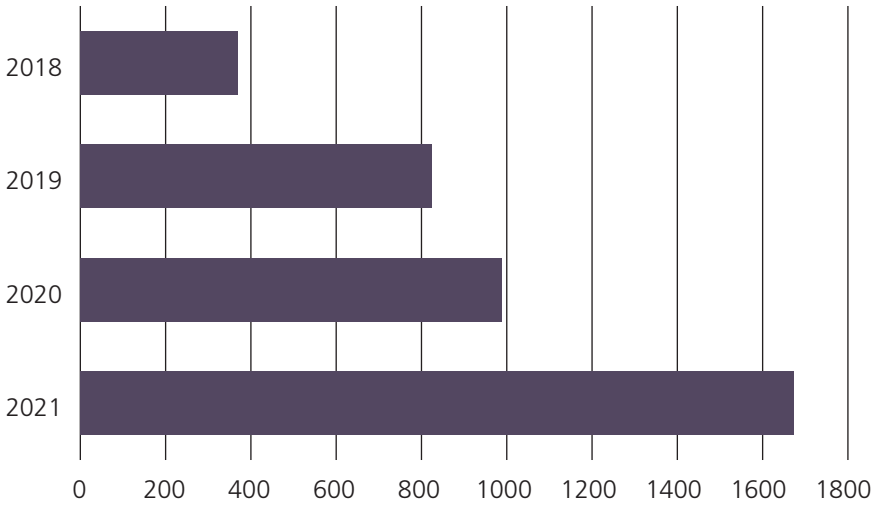
Die Zahl der Beschwerden, die Betroffene gemäß Art. 77 DS-GVO bei der Aufsichtsbehörde einreichen können, stieg im vergangenen Jahr leicht an. Nach 2479 Beschwerden im Jahr 2020 waren es in diesem Berichtszeitraum 2538. Abschließen konnte ich 2531 Beschwerdeverfahren, offen waren zum 31.12.2021 noch 623. Hier sind auch Verfahren berücksichtigt, die vor dem aktuellen Berichtszeitraum in meinem Haus eingegangen sind.



Gemeldete Datenschutzverletzungen

Die gemäß Art. 33 DS-GVO gemeldeten Datenschutzverletzungen nahmen im vergangenen Jahr deutlich zu. Waren es 2020 noch 989, so stieg diese Zahl nun auf 1673. Zum Teil ist dieser immense Anstieg auf die zahlreichen Meldungen zu Microsoft Exchange Severn zurückzuführen (siehe auch J.8.3., S. 168).

Die Zahl der abgeschlossenen Verfahren belief sich in diesem Bereich auf 1785, offen waren zum 31.12.2021 insgesamt 374. Auch hier finden Verfahren Berücksichtigung, die zum Teil vor dem 1.1.2021 eingegangen sind.



Abhilfemaßnahmen nach DS-GVO

Ich habe 2021 eine Warnung (Art. 58, Abs. 2 lit. a DS-GVO), 9 Anweisungen und Anordnungen (Art. 58, Abs. 2 lit. c-h und j) sowie 344 Verwarnungen (Art. 58, Abs. 2 lit. b DS-GVO) ausgesprochen. Von letzteren richteten sich 189 an den nicht-öffentlichen und 155 an den öffentlichen Bereich. Zudem habe ich 42 Bußgeldbescheide erlassen (siehe I.3, S. 88). Die Gesamthöhe der verhängten Bußgelder betrug rund 270.000 Euro.

Gerichtsverfahren

Insgesamt wurden im vergangenen Jahr 36 neue Klage- und Antragsverfahren eröffnet, in denen meine Behörde Partei war. In einem Großteil der Fälle (15) wurde dabei die Abweisung einer Beschwerde moniert. Zudem wurden in neun Fällen meine Abhilfemaßnahmen angefochten.

Entschieden wurden im Berichtszeitraum 38 Klage- und Antragsverfahren, zum größten Teil zugunsten meines Hauses. Am häufigsten wurden Klagen und Anträge zurückgenommen (17), fast genauso oft wurden sie als unbegründet abgelehnt (14). Zudem ergaben sich drei Vergleiche und drei Verweisungen.

Beratungen

Im Jahr 2021 erreichten mich knapp 1600 schriftliche Beratungsanfragen (per Post oder E-Mail), was dem Aufkommen des Vorjahres entspricht. Meine Mitarbeiterinnen und Mitarbeiter bemühen sich weiterhin auch in konkreten Einzelfällen Unterstützung zu leisten, wann immer es ihre Zeit zulässt. Leider ist das aufgrund der nach wie vor dünnen Personaldecke meines Hauses nicht immer möglich.

Europäische Verfahren

Im Jahr 2021 war mein Haus in folgendem Umfang mit europäischen Verfahren befasst:

1. Verfahren mit Betroffenheit (Art. 56): 162
2. Verfahren mit Federführung (Art. 56): 3
3. Verfahrensschritte gem. Kap VII DS-GVO (Art. 60 ff.):
   a. Die LfD hat als betroffene Aufsichtsbehörde einen Beschlussentwurf erhalten: 66 Fälle
      Die LfD hat als betroffene Aufsichtsbehörde einen überarbeiteten Beschlussentwurf erhalten: 14 Fälle
   b. Der LfD wurde als betroffener Aufsichtsbehörde ein finaler Beschlussentwurf vorgelegt: 54 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
2021	4.381	56,17

I.2. Beschwerden und Meldungen von Datenschutzverletzungen

Erneut ist die Zahl der Beschwerden und der Meldungen von Datenschutzverletzungen gestiegen. Erreichten mich 2020 insgesamt knapp 3500 Eingänge dieser Art, waren es im Berichtszeitraum rund 4200. Das Themenspektrum ist dabei wie in den vergangenen Jahren sehr breit.

Die Zahl der Beschwerden gemäß Art. 77 Datenschutz-Grundverordnung (DS-GVO) bewegte sich 2021 mit 2538 Eingängen auf einem ähnlichen Niveau wie im Jahr zuvor. Ich hoffe, dass nach Jahren des stetigen und deutlichen Anstiegs nun in diesem Bereich ein Plateau erreicht ist. Denn durch die Prüfung und Bewertung dieser zahlreichen Einzelfälle werden viele Ressourcen meiner Behörde gebunden, die auch für anlasslose Kontrollen und Beratung genutzt werden könnten und müssten.

Schwerpunkt von Beschwerden

Überwachung von Beschäftigten ohne konkreten Verdacht

Nach wie vor ein Dauerbrenner bei den Beschwerden ist das Thema Videoüberwachung in all seinen Facetten. Dies betrifft sowohl die Überwachung durch Privatpersonen als auch durch Unternehmen. Tendenziell scheinen sich immer mehr Verantwortliche im Recht zu fühlen, wenn sie ihre Beschäftigten angeblich zur Verhinderung und Aufklärung von Diebstählen überwachen, ohne dass ein konkreter Verdacht vorliegt (weitere Informationen zur Videoüberwachung, siehe J.9, S. 171). Ich werde meine Bemühungen zur Aufklärung von Verantwortlichen und Betroffenen deshalb weiter fortsetzen und bei eklatanten Verstößen Bußgelder verhängen.

Im Bereich des Beschäftigtendatenschutzes erreichten mich zudem Beschwerden zur Verarbeitung der sogenannten 3G-Daten durch Arbeitgeber und Arbeitgeberinnen (siehe auch J.1.7, S. 105), zur GPS-Überwachung von Beschäftigten (siehe J.6.5, S. 151), zur Löschung von Bewerbungs- und Beschäftigtendaten sowie zum Auskunftsrecht.

Überhaupt war das Recht auf Auskunft gemäß Art. 15 DS-GVO wieder das Betroffenenrecht, auf das sich die meisten Beschwerden bezogen. Dies zog sich durch alle Bereiche des öffentlichen und nicht öffentlichen Sektors, egal ob in Kommunen, Unternehmen oder Arztpraxen. Nicht umsonst hat der Umfang des Rechts auf Auskunft bereits mehrere höchste Gerichte beschäftigt (siehe F.1, S. 48).

Im Zusammenhang mit den Betroffenenrechten gab es aber auch Konstellationen, in denen bei den Betroffenen unzutreffende Vorstellungen hinsichtlich ihrer Rechte vorhanden waren. Teilweise versuchten betroffene Personen bei zivilrechtlichen Streitigkeiten um unbezahlte Forderungen beispielsweise einen Löschanspruch bei einem Vertragspartner oder einem involvierten Inkassounternehmen geltend zu machen und sich so der Forderung zu entziehen. Ein Löschanspruch ist jedoch nicht voraussetzungslos gegeben. So regelt Art. 17 Abs. 3 lit. e DS-GVO, dass personenbezogene Daten nicht gelöscht werden müssen, wenn sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind, weshalb ich solche Beschwerden als unbegründet zurückweise.

Andererseits war nach wie vor zu beobachten, dass Unternehmen auf die Geltendmachung von Betroffenenrechten überhaupt nicht reagierten. Teilweise trugen sie dann im aufsichtsbehördlichen Verfahren vor, dass durch längere Krankheit eines Mitarbeitenden oder andere, vorrangig zu erledigende, Aufgaben keine Antwort möglich war. Es ist jedoch erforderlich, dass Unternehmen sich so organisieren, dass sie innerhalb der gesetzlichen Fristen auf die Geltendmachung von Betroffenenrechten reagieren können. Dazu gehört, dass eindeutige Zuständigkeiten für die Bearbeitung dieser Ansprüche festgelegt werden, ausreichend Kapazitäten für die fristgerechte Bearbeitung bereitgestellt werden und in Krankheitsfällen Vertretungsregelungen greifen.

Manche Unternehmen reagieren überhaupt nicht

Regelmäßig beschwerten sich Betroffene bei mir auch darüber, dass ihre personenbezogenen Daten ohne Rechtsgrundlage Dritten offengelegt wurden. Auch diese Art des Verstoßes zieht sich durch die meisten Bereiche, die meiner Aufsicht unterstehen. So wurden etwa die Testergebnisse von Corona-Testzentren an falsche Empfänger versendet (mehr dazu unter J.1.6, S. 103). Regelmäßig gingen auch Beschwerden darüber ein, dass Kommunen die personenbezogenen Daten von Betroffenen ohne Einwilligung im Internet offengelegt hatten. Ein großer Teil der Verstöße geschah im Rahmen der Beteiligung der Öffentlichkeit nach dem Baugesetzbuch. Hier besteht die Möglichkeit, Stellungnahmen abzugeben, wovon die Betroffenen Gebrauch gemacht hatten.

In Bezug auf die digitalen Medien bemängelten Betroffene häufig das Tracking auf Webseiten, die unzulässige Veröffentlichung von personenbezogenen Daten sowie fehlende oder fehlerhafte Datenschutzerklärungen. Im Wirtschaftsbereich gingen zudem erneut zahlreiche Beschwerden über E-Mail-Werbung bei mir ein. Häufig machen es Verantwortliche dabei den betroffenen Personen in unzulässiger Weise schwer, ihre Widerspruchsrechte wahrzunehmen (siehe auch J.6.4, S. 149). Außerdem wandten sich Bürgerinnen und Bürger vermehrt an mich, nachdem sie Werbepost von Unternehmen erhalten hatten, zu denen sie in keiner Geschäftsbeziehung stehen. Häufig hatten diese Betroffenen bereits von ihrem Recht auf Auskunft Gebrauch gemacht, um herauszufinden, woher das werbende Unternehmen ihre Adresse hat. Im Anschluss erlebten sie, dass mehrere beteiligte Unternehmen die Verantwortung hin- und herschoben und sich letztlich nicht aufklären ließ, wie die Adressdaten in den Bestand eines Adresshändlers gelangen konnten. Häufig verlor sich die Spur außerhalb der EU. Ich leitete gegen mehrere Unternehmen mit einem auffällig hohen Beschwerdeaufkommen daher umfangreichere Untersuchungen ein, die im Berichtszeitraum jedoch noch nicht abgeschlossen werden konnten.

Werbepost von unbekannten Unternehmen

Schwerpunkt der Meldungen von Datenschutzverletzungen

Starker Anstieg bei Meldungen gem. Art. 33 DS-GVO

Verantwortliche müssen gemäß Art. 33 DS-GVO Datenschutzverletzungen, die ein Risiko für die Rechte und Freiheiten der Betroffenen bergen können, innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde melden. Dieser Pflicht kamen im Berichtszeitraum zahlreiche datenverarbeitende Stellen nach, so dass mich 1673 Meldungen erreichten – ein immenser Zuwachs gegenüber den 989 Meldungen im Jahr 2020. Ein Teil dieses Aufwuchses war auf die vielen Eingänge zu Microsoft Exchange Servern zurückzuführen (siehe J.8.3, S. 168), aber auch ohne diesen Umstand hätten die Meldungen gemäß Art. 33 DS-GVO erneut zugenommen.

Auch hier gibt es Sachverhalte, die sich bereits seit Jahren durch alle Bereiche ziehen. Dies trifft etwa auf den Verlust oder Diebstahl sowie besonders auf den Fehlversand von Daten zu. Ob in der Justizverwaltung, in Unternehmen oder im Gesundheitsbereich – immer wieder gehen Schreiben, E-Mails oder sonstige Unterlagen an die falschen Empfänger. Verantwortliche sollten deshalb, vor allem wenn sie mit besonders sensiblen Daten arbeiten, das Vier-Augen-Prinzip anwenden und für den Versand ausreichende zeitliche Kapazitäten einplanen. Denn in den meisten Fällen sind diese Datenschutzverletzungen auf Flüchtigkeitsfehler zurückzuführen. Ob diese Fehler sämtlich meldepflichtig sind, hängt stark vom Einzelfall ab und muss vom Verantwortlichen bewertet werden, was mitunter durchaus herausfordernd sein kann.

So wurde etwa im Berichtszeitraum von einer Interessenvertretung der Ärztinnen und Ärzte die Frage an den Arbeitskreis Gesundheit und Soziales der Datenschutzkonferenz herangetragen, ob in Fällen des Fehlversands von Gesundheitsdaten von einem Arzt an einen anderen, der nicht an der Behandlung beteiligt ist, auf die Meldung einer Datenschutzverletzung verzichtet werden kann. Da der empfangende Arzt ebenfalls einer gesetzlichen Schweigepflicht unterliege, würde kein Risiko für die Rechte der Betroffenen bestehen. Zudem würde die Meldung in solchen Fällen einen zu hohen bürokratischen Aufwand für die Verantwortlichen darstellen.

Diese Auffassung teile ich nicht. Zunächst gilt die Schweigepflicht des § 203 Strafgesetzbuch nur zwischen dem behandelnden Arzt und dem behandelten Patienten, nicht jedoch zwischen einem Arzt und einem ihm unbekannten dritten Patienten.

Hinsichtlich der Höhe des Risikos für die Betroffenen können - beispielsweise in Fällen eines Fehlversands von Gesundheitsdaten an unbefugte Personen - die weiteren Umstände der empfangenden Person oder Stelle herangezogen werden. Ist der unrechtmäßige Empfänger aufgrund seines Berufes mit dem Umgang mit sensiblen Daten vertraut, weil er gegebenenfalls selbst einer beruflichen Verschwiegenheitspflicht unterliegt und sein Verhalten gegenüber dem Versender daraus schließen lässt, dass die zu Unrecht erhaltenen Daten unverzüglich zurückgesandt oder gelöscht werden, kann dies das Risiko eines Missbrauchs der Daten für die Betroffenen mindern. Das entbindet den Verantwortlichen jedoch nicht von der Meldepflicht an die Aufsichtsbehörde.

Cyber-Attacken nehmen zu

Viele weitere Datenschutzverletzungen gehen auf Cyber-Angriffe zurück. Die Meldungen wegen des Versands von Phishing-Mails und insbesondere der Befall von IT-Systemen mit Verschlüsselungstrojanern nahmen im Berichtszeitraum zu.

Verantwortliche wendeten sich zunehmend an mich, weil sie darauf aufmerksam gemacht wurden, dass von ihren E-Mail-Servern Phishing-Mails versandt wurden. Diese sehen teilweise täuschend echt aus und nehmen Bezug auf bisherigen Mail-Verkehr. So werden unaufmerksame Empfänger schnell dazu verleitet, auf einen Link in der Mail zu klicken oder einen Anhang zu öffnen, wodurch Malware auf den Rechner gelangt. Dies birgt nicht nur erhebliche Risiken für personenbezogene Daten, sondern kann auch den Geschäftsbetrieb oder die Verwaltungsarbeit nachhaltig stören.

Verschlüsselungstrojaner haben sich, wie auch den Medien zu entnehmen ist, zu einem großen Problem für viele Unternehmen und Behörden entwickelt. Die Angreifer beschränken sich nicht immer darauf, die Daten nur zu verschlüsseln. Teilweise werden die Daten auch extrahiert und die Erpresser drohen mit deren Veröffentlichung im Internet. Ein wirksamer Schutz hiergegen wäre die Verschlüsselung der Daten durch die verantwortliche Stelle selbst, was aber zu häufig nicht geschieht.

Leitlinien des EDSA zu typischen Datenschutzverletzungen: https://t1p.de/data-breach

Der Europäische Datenschutzausschuss hat in der Leitlinie 1/2021 typische Datenpannen, dazugehörige Präventionsmaßnahmen und Abhilfemaßnahmen im Nachgang von Datenpannen aufgeführt.

I.3. Überblick über bearbeitete Bußgeldverfahren

Im Jahr 2021 verhängte ich vor allem aufgrund unzulässiger Videoüberwachungen Bußgelder. Mit weiteren Bußgeldverfahren sanktionierte ich unzureichende technische Maßnahmen zum Schutz personenbezogener Daten.

2021 habe ich insgesamt 103 neue Fälle unter Gesichtspunkten einer möglichen Geldbuße geprüft. Im gleichen Zeitraum habe ich 42 Erstbescheide in Bußgeldsachen erlassen, die sich zum Teil auf Fälle bezogen, die bereits im Vorjahr eingeleitet wurden. Von diesen Bescheiden sind 35 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.

Höhe und Adressaten von Geldbußen

Mit Erstbescheiden wurden Geldbußen in Höhe von rund 270.000 Euro festgesetzt. Die Bescheide wurden gegenüber Verantwortlichen aus den Bereichen medizinische Versorgung, Vereinsleben, Einzelhandel, Versandhandel und Tourismus sowie gegen natürliche Personen erlassen. Die natürlichen Personen haben die vorgeworfenen Verstöße teilweise als Inhaber von Unternehmen begangen.

Geahndet wurden Verstöße gegen die Artikel 5, 6, 30, 32, 35 sowie 83 Absatz 5 lit. e Datenschutz-Grundverordnung (DS-GVO) und § 26 Bundesdatenschutzgesetz (BDSG). Dabei handelte es sich um die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage, um die Nichtführung bzw. Nichtvorlage von Verzeichnissen der Verarbeitungstätigkeit, um unzureichende technische Maßnahmen, um die Nichtbeachtung behördlicher Anweisungen sowie um die Verarbeitung beruflicher Daten für private Zwecke.

Gerichtliche Entscheidungen

Im Jahr 2021 wurden durch die Gerichte vier Entscheidungen zu Bußgeldverfahren getroffen. Die Betroffenen haben die Verstöße in der Sache 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. Ein Verfahren aus Vorjahren wurde vom Gericht einvernehmlich mit Staatsanwaltschaft und Verwaltungsbehörde während der Hauptverhandlung eingestellt, da eine Ahndung nicht mehr geboten erschien. Zwei Einsprüche wurden vollständig zurückgenommen, bevor es zu einer gerichtlichen Entscheidung in der Sache kommen konnte.

Weitere gerichtliche Entscheidungen gegen Bußgeldbescheide meiner Behörde stehen aus und werden für das Jahr 2022 erwartet.

Einzelne Fallkonstellationen

Unzulässige Videoüberwachung

Auffallend viele Fälle betrafen auch im Jahr 2021 den Bereich der Videoüberwachung. Dabei lag ein Schwerpunkt erneut auf Verfahren, in denen Arbeitgeber ihre Beschäftigten per Video überwachen (siehe auch J.9.2 und J.9.3, S. 173 ff.). Mein Vorgehen gegen Videoüberwachung am Arbeitsplatz habe ich bereits in den vergangenen Tätigkeitsberichten ausführlich vorgestellt (siehe Tätigkeitsbericht für das Jahr 2019 ab Seite 173 und Tätigkeitsbericht für das Jahr 2020 ab Seite 82).

Unzureichende technische Sicherungsmaßnahmen

In einem sanktionierten Fall wurden Telekommunikations-Hardware, ein Server und die Backup-Technik in einer Gästetoilette untergebracht. Der Server-Schrank, der über kein intaktes Schloss verfügte, hatte eine relativ geringe Höhe und diente zugleich als Wickeltisch. Weder die leichte Zugänglichkeit noch das Risiko für die Verfügbarkeit (Feuchtigkeitsschäden) waren unter Gesichtspunkten der Art. 25, 32 DS-GVO akzeptabel. Nachdem meine Behörde interveniert hatte, wurde zunächst das Schloss des Server-Schrankes ausgetauscht und zeitnah der Schrank mit einer Wand von der restlichen Toilette abgetrennt. Die Geldbuße wurde für den Zustand vor dem Umbau festgesetzt.

Server-Schrank auf dem Wickeltisch

Sanktioniert wurden zudem mehrere Fälle über das Internet zugänglicher Live-Kameras. In einem Fall war die Veröffentlichung von Videoaufnahmen des öffentlichen Raums beabsichtigt, wobei es für den verfolgten Zweck (Werbung) keiner Verarbeitung personenbezogener Daten bedurfte. Die Kameras wurden beanstandet, weil Personen erkennbar waren. Die ergriffenen technischen Maßnahmen waren unzureichend, da in Teilen des Aufnahmebereichs keine Privatsphärenmaskierung (Verpixelung, Schwärzung) vorgenommen worden war.

In einem anderen Fall wurden die Kamerabilder eines Ladengeschäfts ohne Wissen und Wollen des Verantwortlichen verbreitet, mutmaßlich aufgrund einer fehlerhaften Konfiguration. Die Zwecke erforderten die Verarbeitung personenbezogener Daten. Gleichwohl war die Verarbetung zu beanstanden, da Beschäftigte in einem unzulässigen Umfang betroffen waren und auch das nicht öffentlich gesprochene Wort von Kundinnen und Kunden aufgezeichnet wurde. Die Geldbuße wurde insbesondere aufgrund der Veröffentlichung der Aufnahmen verhängt.

Dashcams

Zum Sonderkomplex der Dashcam-Geldbußen habe ich bereits im Tätigkeitsbericht 2019 ausführlich berichtet (S. 105 ff.) und im Oktober 2020 zusätzlich einen umfangreichen Fragen-Antworten-Katalog veröffentlicht. Gleichwohl entfielen auch im Jahr 2021 zahlreiche Bußgeldentscheidungen auf unzulässig eingesetzte Dashcams. Zugleich ist die Zahl der Fälle gestiegen, in denen Aufzeichnungen aus Fahrzeugen heraus auf Internetplattformen veröffentlicht wurden.

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

I.4. Die Verständigung im Bußgeldverfahren

Die Möglichkeit einer einvernehmlichen Verständigung im Bußgeldverfahren durch Erörterung des Vorwurfs und der möglichen Rechtsfolgen wird auch von meiner Behörde in geeigneten Fällen genutzt. Die bisherigen Erfahrungen mit diesem Instrument sind allgemein positiv.

Die aus dem Strafrecht bekannte Absprache zwischen dem Gericht, der Staatsanwaltschaft und der beschuldigten Person zur einvernehmlichen Beendigung des Verfahrens nach § 257c Strafprozessordnung (StPO) kann aufgrund des Verweises auf die strafrechtlichen Vorschriften in § 71 Ordnungswidrigkeitengesetz (OWiG) bzw. § 46 Abs. 1 OWiG auch bei der Entscheidung über ein Bußgeld durchgeführt werden. Dies gilt zugleich für das behördliche, vorgerichtliche Bußgeldverfahren zur Erstellung eines Bußgeldbescheides im Einvernehmen mit dem Verantwortlichen.

Warum Verständigungen im Bußgeldverfahren?

Vorteil: Schnelleres und weniger aufwändiges Verfahren

Die DS-GVO sieht eine effektive Sanktionierung datenschutzrechtlicher Verstöße vor. Meine Behörde ahndet daher regelmäßig aufgedeckte Verstöße mit einem Bußgeld, wenn dies nach der Art und der Schwere angemessen ist. In manchen Fällen erscheint dabei eine einvernehmliche Beendigung des Bußgeldverfahrens passend. Dies sind beispielsweise Verfahren, in welchen einerseits ein schwerer Verstoß zweifellos vorliegt, andererseits eine weitere Aufklärung des konkreten Sachverhalts sehr zeitintensiv und mit erheblichem Aufwand verbunden ist. Weiter handelt es sich um Fälle, in denen durch das Verhalten der beschuldigten verantwortlichen Stelle und der Kommunikation mit meiner Behörde bereits eine mögliche Verständigungsbereitschaft erkennbar ist.

Der Vorteil einer Verständigung liegt für meine Behörde in der schnelleren und weniger aufwändigen Beendigung des Verfahrens unter Schonung der Personalressourcen. Für die Gegenseite bedeutet eine Verständigung oftmals ein niedrigeres Bußgeld und die zügige Beendigung des Verfahrens. Insgesamt ist für die verantwortliche Stelle nach einem Verständigungsgespräch oft der Vorwurf und die Sanktion besser nachvollziehbar und akzeptabel.

Rechtliche Voraussetzungen und Grenzen

Grundlage einer Verständigung ist immer die behördliche Feststellung eines tatsächlich begangenen, bußgeldbewehrten Verstoßes. Daher dürfen keine wesentlichen Fragen zum Sachverhalt oder zur rechtlichen Bewertung offen sein.

Gemäß § 257c Strafprozessordnung soll das Geständnis des bzw. der bußgeldrechtlich Betroffenen Gegenstand der Verständigung sein, welches dann mildernd bei der Bußgeldzumessung berücksichtigt werden kann.

Weiter ist bei einer Verständigung darauf zu achten, dass die vorgeworfene Tat mit einer angemessenen und abschreckenden Sanktion belegt wird. Gegenstand einer Verständigung dürfen im Hinblick auf § 257c StPO nur die Rechtsfolgen einer Sanktionierung sein, also insbesondere die Höhe der festzusetzenden Geldbuße. Dies bedeutet, dass im Rahmen einer Verständigung in der Regel keine weitere Auseinandersetzung über die rechtliche Bewertung einer Tat erfolgt. Gemäß § 257c StPO ist lediglich die Angabe einer Ober- und Untergrenze des angestrebten Bußgeldes zulässig, eine Verständigung auf eine ganz konkreten Bußgeldhöhe scheidet daher aus. Das für die Verständigung wesentliche Geständnis wird verbunden mit der Einigungsbereitschaft

Keine Verständigung auf konkrete Bußgeldhöhe

als mildernder Umstand gewertet, der zu einer Ermäßigung des Bußgeldes führt.

Der bzw. die bußgeldrechtlich Betroffene ist an die Zusagen aus einer Verständigung nicht gebunden, ein Einspruch gegen den Bußgeldbescheid bleibt möglich. Vor dem Hintergrund des Grundsatzes des fairen Verfahrens ist hingegen eine Verpflichtung der Bußgeldbehörde bezüglich des zugesagten Bußgeldrahmens anzunehmen, sofern der bzw. die Betroffene die eigenen Zusagen erfüllt. Diese Bindungswirkung entfällt, wenn sich nach der Verständigung herausstellt, dass tatsächliche oder rechtlich bedeutsame Umstände offenkundig übersehen wurden oder sich neu ergeben haben und der in Aussicht gestellte Bußgeldrahmen dadurch nicht mehr tat- oder schuldangemessen erscheint (vgl. § 257c Abs. 4 StPO).

Ablauf von Verständigungen

Start mit Gespräch zur Erörterung

In geeigneten Fällen unterbreitet meine Behörde der bzw. dem bußgeldrechtlich Betroffenen bereits im Anhörungsschreiben das unverbindliche Angebot eines Erörterungsgespräches mit dem Ziel einer Verständigung. Im Erörterungsgespräch wird dann das geplante weitere Vorgehen, die abstrakte Berechnung der Bußgeldhöhe und in der Regel auch bereits der im konkreten Fall anvisierte Bußgeldkorridor dargestellt. Nach formeller Zustimmung der im Gespräch getroffenen Absprachen wird ein kurzer Bußgeldbescheid mit dem gesetzlichen Mindestinhalt erlassen. Die Erklärung eines Rechtsbehelfsverzichts durch die oder den Betroffenen ist nicht erforderlich, kann sich im Einzelfall aber anbieten, um den Bußgeldbescheid vorzeitig rechtskräftig werden zu lassen. Legt der Betroffene Einspruch gegen den Bußgeldbescheid ein, entfällt der Verständigungsabschlag, und auch eine Verschlechterung im Übrigen ist weder im behördlichen noch im gerichtlichen Verfahren ausgeschlossen.

Nach der bisherigen Erfahrung wird die Möglichkeit eines solchen Erörterungsgespräches von den Betroffenen gerne angenommen, weil es Verantwortlichen die Möglichkeit bietet, ein Ordnungswidrigkeitenverfahren zügig zu beenden und ihre Geständnisbereitschaft bußgeldmindernd berücksichtigt wird. Für meine Behörde wird der Arbeitsaufwand vor allem dadurch reduziert, dass die Verständigung in einen verkürzten Bußgeldbescheid mündet, der nur die gesetzlichen Mindestanforderungen enthält und vor allem eine streitige Auseinandersetzung in einem gerichtlichen Verfahren in der Regel vermieden wird, die weitere Personalressourcen binden würde. Auf diese Weise kommt es überwiegend zu einer für beide Seiten akzeptablen Beendigung des Verfahrens.

I.5. Durchsetzung von Anordnungen gegen öffentliche Stellen im Bereich der DS-GVO

Die Datenschutz-Grundverordnung (DS-GVO) ermöglicht den Erlass von Verwaltungsakten gegen öffentliche Stellen. Die Durchsetzung dieser Verwaltungsakte mit Mitteln des Verwaltungszwangs ist allerdings nach derzeitiger Gesetzeslage nicht möglich.

Das europäische Datenschutzrecht unterscheidet im Anwendungsbereich nicht zwischen privaten und öffentlichen Stellen. Verwaltungsakte gegen Behörden als verantwortliche Stellen (s. Art. 4 Nr. 7 DS-GVO) sind nach der DS-GVO ausdrücklich vorgesehen. Nach dem in Deutschland allgemein geltenden Grundsatz ist jedoch gegen öffentliche Stellen kein Verwaltungszwang möglich. Im Falle einer Weigerung der Behörde, sich gemäß der Verpflichtung eines Verwaltungsaktes zu verhalten, kann der Akt daher grundsätzlich nicht mit den allgemeinen Mitteln des Verwaltungszwangs durch die erlassende Behörde durchgesetzt werden.

Es ist fraglich, ob dies auch für den Bereich der DS-GVO anzunehmen ist oder ob hier aufgrund der Gleichbehandlung von privaten und öffentlichen Stellen Ausnahmen gelten.

Unzulässigkeit der Anwendung von Zwangsmitteln gegen öffentliche Stellen

Öffentliche Verwaltung ist an Recht und Gesetz gebunden

Die öffentliche Verwaltung ist bei Ausübung ihrer Aufgaben an Recht und Gesetz gebunden (Art. 20 Abs. 3 Grundgesetz). Daher wird allgemein erwartet, dass Behörden Hinweisen und formellen Anordnungen von Aufsichtsbehörden ohne weiteren Zwang nachkommen. Hieraus ergibt sich der Grundsatz, dass gegen öffentliche Stellen kein Verwaltungszwang zulässig ist (s. § 17 Verwaltungsverfahrensgesetz für Bundesbehörden und s. die gleichlautenden Regelungen in verschiedenen landesrechtlichen Verwaltungsverfahrensgesetzen).

In Niedersachsen ergibt sich die weitgehende Unzulässigkeit einer Zwangsvollstreckung gegen öffentliche Stellen durch einen Umkehrschluss aus § 64 Abs. 2 S. 3 Niedersächsisches Polizei und Ordnungsbehördengesetz (NPOG) (in Verbindung mit § 70 Abs. 1 Niedersächsisches Verwaltungsverfahrensge-

setz für das allgemeine Verwaltungsrecht): Das Zwangsmittel der Ersatzvornahme kann auch gegen eine juristische Person des öffentlichen Rechts angewendet werden, sofern diese dadurch nicht an der Erfüllung ihrer öffentlichen Aufgaben gehindert wird und sofern die Voraussetzungen des § 64 Abs. 2 S. 1 Nr. 1 NPOG – insbesondere das Vorliegen einer gegenwärtigen Gefahr – erfüllt sind. So ist auch in Niedersachsen die Möglichkeit einer Durchsetzung einer behördlichen Anordnung auf das Mittel der Ersatzvornahme in den wenigen denkbaren Fällen einer unmittelbar vorliegenden Gefahr begrenzt. Insbesondere ist die Verhängung eines Zwangsgeldes ausgeschlossen.

Kein Zwangsgeld möglich

Verwaltungszwang gegenüber Behörden im Bereich des Datenschutzrechts

Da für das Datenschutzrecht und dessen Durchsetzung keine Sonderregelung getroffen wurde, gilt die Regelung des § 64 Abs. 2 S. 3 NPOG auch bei der Anwendung von Verwaltungszwang im Rahmen der DS-GVO. Der niedersächsische Landesgesetzgeber erteilte meiner Forderung nach einer eindeutigen und umfassenden Vollstreckungsbefugnis gegen öffentliche Stellen im Bereich des Datenschutzrechts eine klare Absage: Da alle öffentlichen Stellen an Recht und Gesetz gebunden seien, könne von diesen eine Umsetzung der Entscheidungen der Aufsichtsbehörde im Einzelfall erwartet werden, gegebenenfalls könne das Einschreiten der Rechts- oder Fachaufsicht geprüft werden (LT-Drucksache 18/548, S. 65).

Bei aller Kritik an einem Fehlen der Befugnis zur Vollstreckung der eigenen aufsichtsbehördlichen Maßnahmen kann jedoch nicht von einem eindeutigen Rechtsfehler unter Berücksichtigung der europarechtlichen Vorgaben ausgegangen werden, welcher zur Folge hätte, dass die nationalen Vollstreckungsregelungen im Bereich der DS-GVO nicht zur Anwendung kommen. Denn auch wenn die DS-GVO die Anwendung von aufsichtsbehördlichen Maßnahmen gegen öffentliche Stellen zulässt, trifft sie doch gerade keine Regelung zur Verwaltungsvollstreckung, womit dies dem nationalen Gesetzgeber überlassen ist. Die Voraussetzungen einer Zwangsvollstreckung bestimmen sich daher allein nach niedersächsischem Vollstreckungsrecht.

Ausnahmeregelung nötig

Als Aufsichtsbehörde, welche zum Erlass von Maßnahmen wie Anordnungen auch gegenüber öffentlichen Stellen befugt ist, halte ich nach wie vor die Schaffung einer ausdrücklichen, gesetzlichen Regelung im Sinne eines Ausnahmetatbestandes für den Datenschutzbereich für erforderlich, um unmittelbar eigene Vollstreckungen auch gegen Behörden zu ermöglichen. Die Erfahrung zeigt eben leider doch, dass sich Behörden nicht immer an Recht und Gesetz halten (Beispiel: Meine Aufforderung an die Staatskanzlei zur Abschaltung von Facebook-Fanpages blieb bisher ohne Folge.). Ein mögliches Ein-

schreiten der Rechts- bzw. Fachaufsichtsbehörde ist kein ausreichendes Äquivalent zur Durchsetzung eines Verwaltungsaktes im Wege des Verwaltungszwangs durch die erlassende Behörde selbst. Eine allgemein zugeschnittene verwaltungsrechtliche Aufsichtsbehörde ist weitaus weniger in der Lage zur Einhegung eines datenschutzrechtlichen Problems als die dafür zuständige Datenschutzaufsichtsbehörde. Hinzu kommen denkbare divergierende Rechtsauffassungen von Rechts- bzw. Fachaufsichtsbehörde und Datenschutzaufsichtsbehörde, welche letztlich zumindest zu einer nicht hinnehmbaren Verzögerung bei der Abhilfe eines datenschutzrechtlichen Verstoßes führen können.

Datenschutzkonferenz fordert Erweiterung des BDSG

Die durch die DS-GVO zugestandene Befugnis zur Verhängung von aufsichtsbehördlichen Maßnahmen gegen Behörden sollte durch die Befugnis zu einer Durchsetzung im Wege des Verwaltungszwangs ergänzt werden. Dementsprechend hat es die Datenschutzkonferenz in ihrer Stellungnahme zur Evaluierung des Bundesdatenschutzgesetzes (BDSG) für dringend erforderlich gehalten, die aufsichtsbehördlichen Befugnisse im BDSG zu erweitern (siehe E.8, S. 45), indem gegenüber öffentlichen Stellen die Durchsetzung von Maßnahmen mit Zwangsmitteln sowie die Anordnung der sofortigen Vollziehung ermöglicht wird.

J. Aktuelle Themen

J.1. Datenschutz und Corona

1.1 Änderung und Neufassung der Niedersächsischen Corona-Verordnung

Eine gute datenschutzrechtliche Beratung setzt meine frühzeitige Einbindung bei Rechtsetzungsvorhaben voraus – dies war bei der Niedersächsischen Corona-Verordnung leider nicht der Fall.

Im Jahr 2021 wurde die Niedersächsische Corona-Verordnung mehrfach geändert oder neu gefasst. Eine Vielzahl der Regelungen hat datenschutzrechtliche Relevanz. Obwohl die Landesregierung in ihrer Stellungahme vom 18. Juni 2020 zu der Kleinen Anfrage „Spricht das Sozialministerium mit der Datenschutzbeauftragten?“ (Drs.18/6773) erklärt hatte, dass meine Behörde bei datenschutzrechtlich relevanten Maßnahmen stets eingebunden wird, fand dies im Berichtszeitraum bei den entsprechenden Verordnungsänderungen nicht statt.

Antwort zur Kleinen Anfrage: https://t1p.de/anfrage-ms

Oft habe ich von Regelungen mit Datenschutzbezug erst durch die Veröffentlichungen im Niedersächsischen Gesetz- und Verordnungsblatt erfahren. Das ist nicht nur im Hinblick auf den mir obliegenden Beratungsauftrag von Parlament und Landesregierung nach Art. 57 Abs. 1 Buchstabe c) DS-GVO misslich, sondern erschwert zugleich die datenschutzrechtliche Beratung der betroffenen öffentlichen und nicht-öffentlichen Stellen in Niedersachsen beim Vollzug der Verordnung. Zum Teil weist die Verordnung aber auch inkonsistente Regelungen auf, die bei einer frühzeitigen Einbindung meiner Behörde hätten vermieden werden können.

Ich habe das für die Verordnung zuständige Sozialministerium im Oktober 2021 erneut angeschrieben und die in der DS-GVO sowie der Gemeinsamen Geschäftsordnung der Landesregierung und der Ministerien vorgesehene frühzeitige Einbindung meiner Behörde bei datenschutzrelevanten Rechtsänderungen eingefordert. Eine Rückantwort des Sozialministeriums habe ich im Berichtszeitraum nicht erhalten.

1.2 Einsatz der Luca-App in Niedersachsen

Niedersachsen war eines der 13 Bundesländer, die sich zur Umsetzung der Kontaktnachverfolgung für den Einsatz der Luca-App entschieden haben (siehe auch E.1, S. 29). Die App sollte die niedersächsischen Gesundheitsämter bei der Kontaktnachverfolgung infizierter Personen unterstützen, indem sie medienbruchfrei die digitale Kontaktdatenerfassung und unmittelbare Übernahme in die eigenen Verarbeitungssysteme ermöglicht.

Am 3. März 2021 beschlossen die Ministerpräsidentinnen und Ministerpräsidenten gemeinsam mit der Bundeskanzlerin die dringliche Vergabe einer Infrastruktur zur digitalen Kontaktnachverfolgung. Diese Entscheidung wurde gefällt, um den Lock-Down zu beenden und gleichzeitig das Risiko einer erneuten Welle der Corona-Pandemie möglichst geringzuhalten. In Niedersachsen und zwölf weiteren Ländern fiel die Vergabeentscheidung zugunsten der Luca-App der culture4life GmbH aus. Die App ermöglichte es den nach der niedersächsischen Corona-Verordnung verpflichteten Stellen, die Kontaktdaten von Besucherinnen und Besuchern oder Teilnehmenden digital zu erfassen. Des Weiteren konnten die Gesundheitsämter von infizierten Personen, die die Luca-App nutzten, eine Besuchshistorie abfragen. Im Anschluss konnten sie von Veranstaltern, bei denen sich die infizierten Personen aufgehalten hatten, für relevante Zeiträume Gästelisten anfordern. Sowohl die Besuchshistorie als auch die Gästelisten konnten über die Luca-App an das anfragende Gesundheitsamt übermittelt und in das in Niedersachsen zur Kontaktnachverfolgung eingesetzte System SORMAS übernommen werden.

Zu SORMAS siehe Tätigkeitsbericht 2020, Kapitel J.1.5: https://t1p.de/2020-tb

Die Luca-App wies gegenüber anderen Apps zur digitalen Kontaktnachverfolgung die Besonderheit auf, dass die Gesundheitsämter technisch direkt in das System eingebunden waren. Das Geschäftsmodell richtete sich nicht an die Veranstalter, die die Luca-App zur Erfüllung der ihnen auferlegten rechtlichen Pflichten einsetzten, sondern an die für die Gesundheitsämter zuständigen Landesministerien. Das Land Niedersachsen schloss im März 2020 mit der culture4life GmbH einen Kooperationsvertrag für den Einsatz von Luca.

Innenministerium bittet um Rat

Stellungnahmeder DSK: https://t1p.de/Stellungnahme-Kontaktnachverfolgung

Das Niedersächsische Ministerium für Inneres und Sport unterrichtete mich am 30. April 2021 schriftlich über den Einsatz des Luca-Systems in Niedersachsen und bat um Hinweise für den datenschutzgerechten Einsatz. Zu diesem Zeitpunkt hatten mich bereits zahlreiche Beratungsanfragen von Veranstaltern zur Datenschutzkonformität der Luca-App erreicht. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) hatte in ihrer Stellungnahme vom 26. März 2021 „Kontaktnachverfolgung in Zeiten der Corona-Pandemie: Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden“ auf konkrete datenschutzrechtliche Risiken des Luca-Systems hingewiesen.

Gegenüber dem Ministerium wies ich darauf hin, dass das Kontaktnachverfolgungssystem Luca zeitgleich in mehreren Ländern Gegenstand datenschutzaufsichtlicher Untersuchungen der jeweiligen Datenschutzaufsichtsbehörden sei. Die DSK hatte daher eine länderübergreifende Taskforce zur Überprüfung der Luca-App gegründet. Aufgrund des Firmensitzes des Unternehmens culture4life GmbH in Berlin gab die Berliner Beauftragte für den Datenschutz und die Informationsfreiheit das Prüfergebnis der DSK an die culture4life GmbH weiter und forderte aufgrund festgestellter datenschutzrechtlicher Defizite Anpassungen.

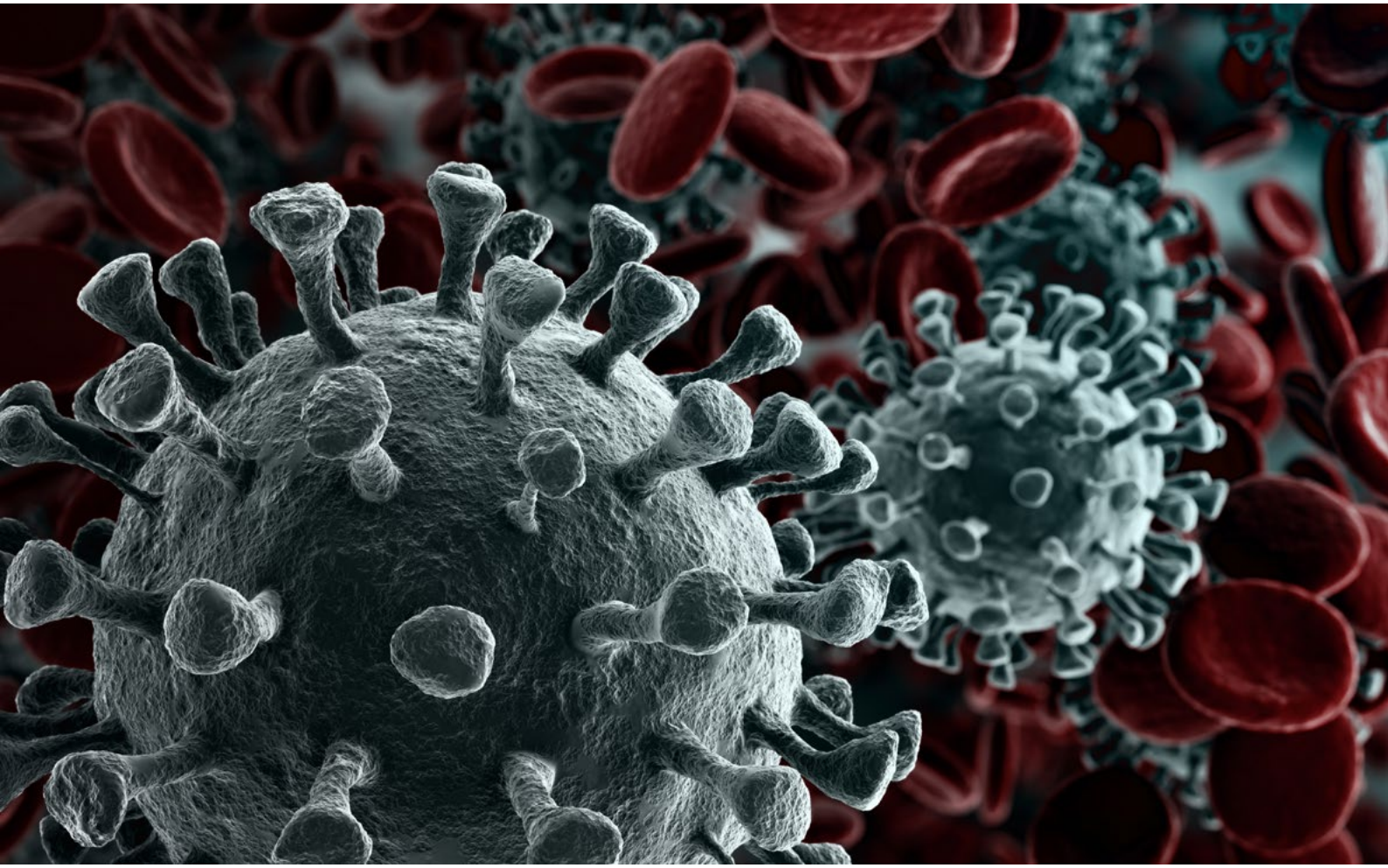
Land verpflichtet sich zur Bewerbung des Systems

Verantwortlichkeit liegt bei Veranstaltern

Ungeachtet des Unternehmenssitzes trug das Land Niedersachsen aufgrund des abgeschlossenen Kooperationsvertrages für den Einsatz des Kontaktnachverfolgungssystems die Verantwortung für dessen datenschutzgerechten Einsatz. Davon zu trennen war allerdings die Bewertung der datenschutzrechtlichen Verantwortlichkeit im Sinne von Art. 4 Nr. 7 DS-GVO. Da die niedersächsischen Gesundheitsämter selbst keine personenbezogenen Daten mit Hilfe der Luca-App verarbeiteten, waren weder diese noch das Land Niedersachsen Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO. Datenschutzrechtlich Verantwortlich für den Einsatz waren Veranstalter, die das System zur digitalen Kontaktdatenerfassung einsetzten. Die Betreiber der Luca-App führten die Datenverarbeitung im Auftrag der Veranstalter durch.

Das Land Niedersachsen verpflichtete sich in der Kooperationsvereinbarung mit culture4life dazu, das Luca-System in angemessener Weise einer breiten Öffentlichkeit bekannt zu machen. Zudem wurde in § 5 Abs. 1 Satz 7a Nds. Corona-Verordnung in der Fassung vom 27. März 2021 eine Regelung eingefügt, nach der die Verpflichtungen zur Datenerhebung und Dokumentation von Veranstaltern entfallen, wenn eine zur Verfügung gestellte Anwendungssoftware genutzt wird, mit der Kontaktdaten sowie Erhebungsdatum und -uhrzeit sowie Aufenthaltsdauer erfasst und an das zuständige Gesundheitsamt übermittelt werden können. Diese zweite Voraussetzung wurde in der Praxis ausschließlich von der Luca-App erfüllt, sodass diese Ergänzung allein deren Verbreitung diente.

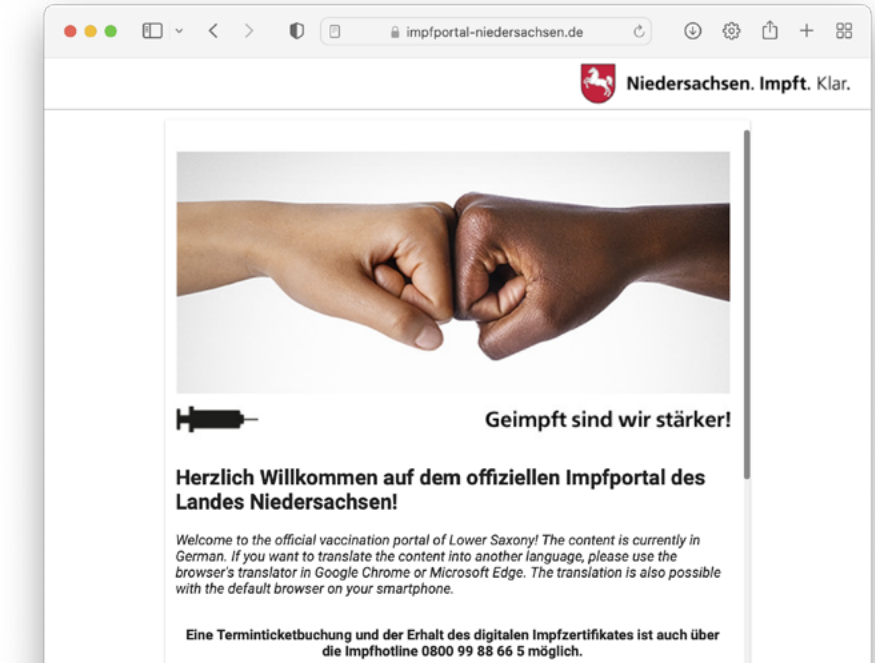
Durch diese Maßnahmen erweckte das Land Niedersachsen bei Veranstaltern den Eindruck, der Einsatz der Luca-App sei datenschutzrechtlich unbedenklich, obwohl dies nicht zutraf. Daher hatte ich dem Niedersächsischen Ministerium für Inneres und Sport dringend geraten, gegenüber dem Kooperationspartner culture4life GmbH mit Nachdruck darauf hinzuwirken, dass die festgestellten datenschutzrechtlichen Defizite schnellstmöglich behoben werden. Im Fokus standen



hierbei insbesondere die Speicherung der gesammelten Daten an einer zentralen Stelle und die Verbesserung des Verschlüsselungskonzeptes. Aus Sicht des Datenschutzes wäre ein dezentrale Datenspeicherung vorzugswürdig, da die unbefugte Einsicht in die großen Datenbestände je nach Umfang zu einer schweren Beeinträchtigung für die Einzelnen und sogar das Gemeinwesen führen kann.

Dieses Beispiel zeigt deutlich, dass politische und ministerielle Entscheidungen häufig weitreichende rechtliche und auch datenschutzrechtliche Konsequenzen haben können. Ich würde mir daher wünschen, dass die niedersächsischen Ministerien mich viel häufiger und möglichst frühzeitig in ihre Entscheidungsprozesse einbeziehen, damit ich ihnen beratend zur Seite stehen kann.

1.3 Datenpanne beim niedersächsischen Impfportal



Im Mai 2021 meldete mir das Niedersächsische Sozialministerium eine Datenschutzverletzung gemäß Art. 33 DS-GVO im niedersächsischen Impfportal. Ein anonymer Hinweisgeber hatte das verantwortliche Ministerium zuvor auf eine Sicherheitslücke in dem Buchungsportal für Impftermine gegen COVID-19 aufmerksam gemacht.

Daten von 1258 Betroffenen abgerufen

Der Hinweisgeber bezeichnete sich als ethischen „White-Hat"-Hacker, der keine bösartigen Absichten verfolgen würde und lediglich eine Schließung der Lücke herbeiführen wolle.
Durch eine nicht für Benutzerinnen und Benutzer vorgesehene Schnittstelle war es dem Hacker möglich gewesen, die Datenbank des Portals nach Parametern zu durchsuchen und dadurch personenbezogene Datensätze von insgesamt 1.258 für einen Impftermin registrierten Personen abzurufen.

Nach Aussage des betreuenden IT-Dienstleisters konnte die Schnittstelle noch am Tag des eingegangenen Hinweises durch eine Einschränkung der Zugriffsberechtigungen geschlossen werden. Die Sicherheitslücke sei über den Abruf des Hackers hinaus nicht weiter ausgenutzt worden.
In Absprache mit dem Sozialministerium wurden die Ursachen für den Vorfall festgehalten und die darauffolgenden Anpassungen des Berechtigungskonzepts als angemessen bewertet. Das Prüfverfahren wurde anschließend eingestellt.

1.4 Datenschutzwidrige Videokonferenzsysteme nicht länger geduldet

Während des ersten Lockdowns und der damit einhergehenden Schließungen hatte ich im Frühjahr 2020 zeitlich begrenzt geduldet, dass öffentliche Stellen (unter anderem Schulen) digitale Kommunikationsmittel – darunter auch Videokonferenzsysteme – einsetzten, die nicht im vollen Umfang sämtliche datenschutzrechtlichen Anforderungen erfüllten. Diese Duldung hatte ich im Herbst 2020 widerrufen.

In der Folge habe ich im Berichtszeitraum den Niedersächsischen Kultusminister als Leiter der obersten Schulbehörde schriftlich darum gebeten, den Einsatz nicht datenschutzkonformer Videokonferenzsysteme in Schulen per Erlass zu unterbinden und die ihm nachgeordneten Bereiche über meine Rechtsauffassung zeitnah zu informieren. Zeitgleich habe ich alle 19 niedersächsischen Hochschulen darüber informiert, dass der Einsatz offenkundig nicht datenschutzkonformer Videokonferenzsysteme im Bildungsbereich von mir nicht weiter geduldet wird und um Anpassung der Verfahren zum datenschutzkonformen Einsatz von Videokonferenzsystemen gebeten. Leider habe ich im Berichtszeitraum keine Antwort des Kultusministers erhalten.

Um die verantwortlichen Stellen – insbesondere die Hochschulen und Schulen – bei der Etablierung datenschutzkonformer Videokonferenzsysteme zu unterstützen, habe ich die bestehenden allgemeinen FAQ zu Videokonferenzsystemen um spezielle FAQ für den Einsatz von Videokonferenzsystemen in Schulen ergänzt (siehe J. 5.2, S. 138).

1.5 2G-Armbänder an niedersächsischen Hochschulen

Im Berichtszeitraum haben mich Anfragen zur Umsetzung der „3G-Regelung" der Niedersächsischen Corona-Verordnung erreicht. Diese Regelung besagt, dass der Zutritt zu bestimmten Einrichtungen unter bestimmten Voraussetzungen nur auf geimpfte, genesene oder getestete Personen beschränkt werden muss.

Um die 3G-Regelung im Studienbetrieb praktikabel zu machen und die Kontrolle zu erleichtern, hat sich eine Hochschule dazu entschieden, für geimpfte und genesene Studierende sowie Beschäftigte der Hochschule farbig markierte Armbänder zur Verfügung zu stellen. Durch Tragen eines Armbandes wird äußerlich erkennbar, dass Studierende oder Beschäftigte entweder genesen oder geimpft sind, ohne dass klar wird, welchen Status sie genau haben. Die Ausgabe der Armbänder erfolgt gegen Vorlage des entsprechenden Nachweises. Eine Dokumentation, dass der Nachweis vorgelegen hat oder die Speicherung weiterer personenbezogener Daten findet hierbei nicht statt.

Gesetzliche Rechtsgrundlage oder Einwilligung nötig

Bei der Erhebung des Nachweises sowie bei der Sichtprüfung des Armbandes werden personenbezogene Daten verarbeitet. Hierfür bedarf es entweder einer gesetzlichen Rechtsgrundlage oder der vorherigen Einwilligung der betroffenen Person.

Erhebung von Nachweisen

In Ermangelung einer gesetzlichen Rechtsgrundlage konnte die Erhebung personenbezogener Daten in Form der Nachweise bei Studierenden und Beschäftigten zunächst nur auf Einwilligungsbasis erfolgen. Hierbei ist entscheidend, dass die Einwilligung auf freiwilliger Basis erfolgt und die betroffenen Personen keinen rechtlichen Nachteil erleiden, falls sie nicht einwilligen. Eine solche Einwilligung wäre auch wirksam, da eine Wahl zwischen den Arten von Nachweisen (Impf-, Genesenen- oder Testnachweis) besteht. Studierende können so Zugang zu Präsenzvorlesungen in der Universität erhalten. Bei Beschäftigten kann zudem die Tätigkeit in einem geschützten Arbeitsumfeld als Vorteil gewertet werden.

Kein Nachteil, falls Einwilligung abgelehnt wird

Im Verlauf des Berichtsjahres hat der Bundesgesetzgeber mit § 28b Infektionsschutzgesetz eine Regelung geschaffen, die die Erhebung des Nachweises über eine Impfung, Genesung oder negative Testung von Beschäftigten durch den Arbeitgeber erlaubt. Die Erhebung entsprechender Nachweise von Studierenden kann zwischenzeitlich auf § 8 Nds. Corona-Verordnung gestützt werden.

Armband? Klar, aber freiwillig!

Das Tragen eines Armbandes zum Zeichen, dass ein Nachweis bereits vorgelegen hat, ist jedoch in allen Fällen nur auf Einwilligungsbasis zulässig. Eine solche Einwilligung wäre auch freiwillig, da es den Studierenden und Beschäftigten freisteht, alternativ stets einen der drei Nachweise beim Einlass vorzuzeigen.

1.6 Eingaben und Beschwerden zu Impf- und Testzentren

In der Corona-Pandemie kommt sowohl Testzentren als auch Impfzentren eine große Bedeutung zu. Zahlreiche Eingaben in diesem Bereich belegen die hohe Sensibilisierung in der Bevölkerung für den Umgang mit Gesundheits- und weiteren personenbezogenen Daten.

Bezogen auf Testzentren betrafen einige Meldungen den Versand von Corona-Testergebnissen an falsche Empfänger. Ein weiterer häufig auftretender Beschwerdegegenstand waren über das notwendige Maß hinausgehende Datenerhebungen, beispielsweise das Erfassen der Personalausweisnummer oder der Krankenkassendaten. Ein dritter Streitpunkt war die Dauer der Datenspeicherung. Manche Bürgerinnen und Bürger verlangten eine augenblickliche Löschung der Daten. Allerdings sind die Testzentren gem. § 7 Absatz 5 Coronavirus-Testverordnung zu einer Speicherung von Nachweisdaten bis zum 31. Dezember 2024 verpflichtet.

Systemische gravierende Mängel, die eine Mehrzahl von Impf- oder Testzentren gleichermaßen betroffen hätten, habe ich jedoch zu keinem Zeitpunkt festgestellt.

Verdacht auf Abrechnungsbetrug im Testzentrum

Kopie des Personalausweises als Testvoraussetzung

Aus den zahlreichen Beschwerden gegen Corona-Testzentren stach besonders die Beschwerde gegen ein Testzentrum hervor, welches von einem Pflegezentrum betrieben wurde. Inhalt der Beschwerde war, dass das Testzentrum als zwingende Voraussetzung für Tests forderte, den Personalausweis und die Krankenkassenkarte zu kopieren.

Ich schrieb das Testzentrum an, woraufhin sich die Geschäftsführerin telefonisch meldete und angab, man habe nur in den Anfangszeiten Kopien angefertigt, da die Rechtslage unklar und alles ein wenig provisorisch gewesen sei. Man fertige nun keine Kopien mehr an und habe vorhandenen bereits vernichtet. Ich habe die Geschäftsführerin darum gebeten, diesen Vortrag noch einmal schriftlich zu bestätigen. Am Folgetag erreichte mich eine E-Mail, in der sich die Geschäftsführerin auf die ärztliche Schweigepflicht berief und jegliche Auskunft verweigerte.

Kurze Zeit später meldeten sich unabhängig voneinander eine ehemalige Mitarbeiterin und Nachbarn des Testzentrums. Sie gaben übereinstimmend an, dass die Geschäftsführerin zahlreiche Kopien von Personalausweisen und Krankenkassenkarten in den benachbarten Papiermülltonnen entsorgt habe, ohne sie vorher zu schreddern. Die ehemalige Mitarbeiterin gab zudem an, dass die Geschäftsführerin die Corona-Tests doppelt abgerechnet habe. Die Nachbarn sandten mir ein ganzes Paket mit schätzungsweise 1.000 Blatt Farbkopien von Personalausweisen und Krankenkassenkarten zu.

Aufgrund der Sachlage, insbesondere des Verdachts auf Abrechnungsbetrug, habe ich diesen Fall an die zuständige Strafverfolgungsbehörde abgegeben.

Überprüfung der Impfberechtigung

Impfzentrum fordert Kopie des Mutterpasses

Vereinzelt erreichten mich auch zu Impfzentren datenschutzrechtliche Meldungen. Dort wurde zu Beginn der Impfkampagne teilweise etwas zu genau geprüft, ob eine Impf-Berechtigung vorlag. In einem Fall bestand ein Impfzentrum beispielsweise auf der Nennung des Entbindungsdatums einer Schwangeren sowie auf einer Kopie des Mutterpasses. In dieser Konstellation hätte das Vorzeigen des Mutterpasses und ein Vermerken der Impfberechtigung genügt.

In einem anderen Fall hatte ein Impfzentrum eigenmächtig einen früheren Arbeitgeber der betroffenen Person kontaktiert. Die betroffene Person hatte zuvor im Impfzentrum behauptet, in einer Arztpraxis tätig zu sein; hieraus hätte sich die Berechtigung zu einer Impfpriorisierung ergeben. Die dabei vorgelegten Dokumente führten allerdings zu Unstimmigkeiten, weshalb durch das Impfzentrum telefonisch Kontakt zu der Arztpraxis aufgenommen wurde, um sich die Impfberechtigung bestätigen zu lassen. Hierfür fehlte es jedoch an einer Rechtsgrundlage. In beiden Fällen habe ich gegenüber den Impfzentren Maßnahmen ergriffen und einen Hinweis auf datenschutzkonformes Handeln gegeben sowie eine Verwarnung aufgrund eines Datenschutzverstoßes ausgesprochen.

1.7 Corona im Beschäftigungsverhältnis

Die Corona-Pandemie beeinflusste im vergangenen Jahr das öffentliche Leben nach wie vor stark. Entsprechend der Entwicklung der Pandemie änderten sich häufig und kurzfristig gesetzliche Regelungen. Viele dieser Regelungen waren mit einer Verarbeitung von personenbezogenen Daten verbunden, insbesondere Gesundheitsdaten. Dementsprechend erreichten mich zahlreiche Anfragen Verantwortlicher sowie Beschäftigter, zudem von Letzteren auch vielfach Beschwerden. Deren Bearbeitung bildet in diesem Berichtszeitraum erneut einen Schwerpunkt für den Bereich Beschäftigtendatenschutz meiner Behörde.

Im Schwerpunkt ging es bei den Fragen sowie den Beschwerden, die mich erreichten, um die Verarbeitung von Gesundheitsdaten der Beschäftigten. Deren Verarbeitung ist untersagt und nur unter sehr engen gesetzlichen Voraussetzungen erlaubt (Artikel 9 Absatz 1 und 2 DS-GVO). Bereits in meinem Tätigkeitsbericht für das Jahr 2020 habe ich im Zusammenhang mit der Corona-Pandemie allgemeine Hinweise zur Verarbeitung von Gesundheitsdaten Beschäftigter erteilt.

Tätigkeitsbericht 2020: https://t1p.de/TB2020

Keine Verarbeitung von 3G-Daten ohne ausdrückliche gesetzliche Grundlage
Im Verlauf der Pandemie ist die Verarbeitung von 3G-Daten, insbesondere von Beschäftigten, immer mehr in den Fokus gerückt. Der Begriff 3G bezeichnet verkürzt, ob eine Person gegen das Coronavirus SARS-CoV-2 geimpft, von diesem genesen oder aber auf dieses getestet ist.

Bei vielen Arbeitgeberinnen und Arbeitgebern bestand und besteht weiterhin das Bedürfnis nach einer Verarbeitung des jeweiligen 3G-Status ihrer Beschäftigten, insbesondere ob es sich bei diesen um Geimpfte oder Genesene handelt (2G). Mir gegenüber wurden unterschiedliche Zwecke genannt, für die eine Verarbeitung insbesondere des Status „Geimpft" erforderlich sei:

- Erfüllung der Arbeitsleistung durch Beschäftigte vor Ort in den Betriebsstätten statt im Home-Office;
- Räumliche Gegebenheiten in den Betriebsstätten, die eine Einhaltung gesetzlicher Abstandsbestimmungen erschweren („1,5-Meter-Regelung", § 2 Absatz 1 Satz 2 der Niedersächsischen Corona-Verordnung vom 23. November 2021);
- Planung von gemeinsamen Arbeitseinsätzen Beschäftigter, zum Beispiel räumliche Zusammenarbeit ausschließlich Geimpfter, Zusammensetzung von Pflegeteams zum Beispiel ausschließlich aus Geimpften;

- Anpassung des betrieblichen Hygienekonzeptes, wobei sogar an einer Betriebsstätte überlegt wurde, bei Geimpften auf die Mund-Nase-Bedeckung zu verzichten. Dies war allerdings bereits aufgrund § 4 Absatz 1 Satz 1 der Niedersächsische Corona-Verordnung unzulässig.

Beschluss Verarbeitung des Impfstatus durch Arbeitgeber: https://t1p.de/Impfstatus-verabreitung-durch-Arbeitgeber

Außer in gesetzlich ausdrücklich geregelten Fällen – wie beispielsweise im Gesundheitsbereich (§ 23 und § 23a des Infektionsschutzgesetzes (IfSG)) – bestand für weitere Arbeitgeberinnen und Arbeitgeber zunächst keine ausdrückliche Rechtsgrundlage, die eine Verarbeitung der 3G-Daten ihrer Beschäftigten generell zuließ. Dies änderte sich erst mit dem Erlass des § 28b IfSG. Davor war die Verarbeitung des 3G-Status von Beschäftigten – unabhängig von deren Erforderlichkeit für die oben genannten Zwecke – durch Arbeitgeberinnen und Arbeitgeber ohne eine freiwillige und damit rechtswirksame Einwilligung der Betroffenen regelmäßig datenschutzwidrig. Die Datenschutzkonferenz (DSK) stellte in ihrem Beschluss „Verarbeitung des Datums „Impfstatus" von Beschäftigten durch die Arbeitgeberin oder den Arbeitgeber" vom 19. Oktober 2021 fest, dass für die Verarbeitung des Impfstatus durch Arbeitgeberinnen und Arbeitsgeber eine gesetzliche Grundlage erforderlich ist.

Verarbeitung von 3G-Daten nach Erlass des Infektionsschutzgesetzes

Anwendungshilfe der DSK: https://t1p.de/FAQ-Beschaeftigtendaten-Corona

Aber auch nach Erlass des § 28b IfSG blieb die rechtskonforme Verarbeitung von 3G-Daten der Beschäftigten für Arbeitgeberinnen und Arbeitgeber eine Herausforderung. Denn diese Regelung ist stark auslegungsbedürftig. Eine Unterstützung für Verantwortliche und Betroffene bietet die Anwendungshilfe „Häufige Fragestellungen nebst Antworten zur Verarbeitung von Beschäftigtendaten im Zusammenhang mit der Corona-Pandemie" der DSK vom 20. Dezember 2021. Damit soll den Verantwortlichen eine datenschutzkonforme Verarbeitung und den Betroffenen die Möglichkeit zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung erleichtert werden.

Impfangebote durch Arbeitgeberinnen und Arbeitgeber

Teilweise organisierten Arbeitgeberinnen und Arbeitgeber für ihre Beschäftigten Impftermine. Beschäftigte wandten sich in diesen Fällen insbesondere mit Anfragen an mich, wenn die Organisation des Impftermins mit einer Offenlegung von konkreten Gesundheitsdaten verbunden war: zum Beispiel durch die Aufforderung, für die Impfung einen Anamnesebogen auszufüllen und diesen der Personalabteilung zur Weiterleitung an die Impfstelle vorzulegen. Den Betroffenen wurde in diesen Fällen geraten – in Absprache mit ihrer Personalabteilung – die Anamnesebögen selbst an die Impfstelle zu übermitteln oder diese der Personalabteilung in einem verschlossenen Umschlag zur Verfügung zu stellen. Im Übrigen bietet die genannte Anwendungshilfe auch für die Organisation solcher Impftermine Unterstützung für Verantwortliche und Betroffene.

1.8 Schreiben zur Impfreihenfolge verunsichern Adressaten

Anfang 2021 wurde der erste Impfstoff zur Bekämpfung der Corona-Pandemie bereitgestellt. Aufgrund der Impfstoffknappheit wurden Priorisierungen der Impfreihenfolge festgelegt. Einzelne Bevölkerungsgruppen waren also früher als andere zur Impfung berechtigt. Die Information der Berechtigten verlief in mehrerlei Hinsicht alles andere als optimal.

Zur Gruppe der höchsten Impfpriorität gehörten Menschen ab 80 Jahren. Zahlreiche Bürgerinnen und Bürger erhielten im Januar einen Brief, dessen Absender die Deutsche Post Direkt GmbH mit Sitz in Nordrhein-Westfalen war, und der offenkundig über 80-jährige Menschen in Niedersachsen erreichen sollte. Der Brief enthielt ein Musterschreiben, das durch seinen Briefkopf den Eindruck erwecken sollte, dass die Sozialministerin persönlich geschrieben habe, und informierte über die bevorstehende Impfmöglichkeit für über 80-jährige Menschen. Tatsächlich erhielten jedoch Menschen verschiedener Altersgruppen, beispielsweise auch unter 50-Jährige das Schreiben.

Die Absendung durch die Deutsche Post Direkt GmbH und die Tatsache, dass oftmals auch jüngere Menschen Adressat des Briefes waren, sorgte für zahlreiche Eingaben bei mir.

Keine Zugangsmöglichkeit des Sozialministeriums zur Datenbank der Deutsche Post Direkt GmbH

Alter anhand von Vornamen geschätzt

Als Grund für die große Streubreite der Briefe wurde bekannt, dass das Alter der Adressaten teilweise anhand ihrer Vornamen geschätzt worden war und daher auch jüngere Menschen angeschrieben wurden. Meine Prüfung ergab außerdem, dass das Niedersächsische Ministerium für Soziales, Gesundheit und Gleichstellung (MS) zu keinem Zeitpunkt eine Zugangsmöglichkeit zur Adressdatenbank der Deutsche Post Direkt GmbH hatte. Vielmehr war allein die Deutsche Post Direkt GmbH datenschutzrechtlich Verantwortliche. Das MS hatte die Kampagne angestoßen und gegenüber der GmbH das Ziel ausgegeben, dass diese in eigener Verantwortung Adressen aus ihrer Datenbank anschreiben sollte, die möglichst innerhalb der Zielgruppe von über 80-Jährigen in Niedersachsen liegen. Als Inhalt der Briefe wurde das bereits erwähnte Musterschreiben des MS verwendet. Dadurch wich der Briefkopf, der die Sozialministerin auswies, vom tatsächlich verantwortlichen Absender ab.

In rechtlicher Hinsicht erfolgte zu keinem Zeitpunkt eine Datenverarbeitung durch das MS. Dem Ministerium war daher kein datenschutzrechtliches Fehlverhalten vorzuwerfen. Allerdings konnte ich die Verwunderung der ange-

schriebenen Bürgerinnen und Bürgern über die Kooperation des Sozialministeriums mit einem eigenständigen Adressdatenbetreiber nachempfinden.

Versand mit Meldedaten wäre möglich gewesen

Meine Irritation wurde durch folgenden Umstand verstärkt: Als die Kampagne in der Öffentlichkeit mit Unverständnis diskutiert wurde, begegnete das MS der Diskussion mit der Aussage, dass eine Nutzung von Meldedaten rechtlich bzw. aufgrund des damit verbundenen Aufwands nicht in Betracht gekommen sei. Damit erweckte das Ministerium öffentlich den Eindruck, dass Datenschutz die Nutzung von Meldedaten für diesen Zweck verhindert hätte. Das war falsch.

Datenschutz stand Verwendung der Meldedaten nicht im Weg

Zum einen hätte das Musterschreiben über die Kommunen versandt werden können: Die Kommunen halten die nötigen Meldedaten ohnehin vor und dürfen sie zu diesem Zweck auch verwenden. Zudem hätte das Sozialministerium die Daten auch über eine sogenannte Gruppenauskunft von den jeweiligen Kommunen erhalten und für die Impfinformation verwenden können. Aus datenschutzrechtlicher Sicht bestand daher keine Notwendigkeit, eine Altersschätzung und Versendung durch die Deutsche Post Direkt GmbH zu veranlassen.

Schreiben an Versicherte mit Vorerkrankungen

Trotz der öffentlichen Diskussion um die erste Informationskampagne sorgte das Sozialministerium nur drei Monate mit einem weiteren missverständlichen Schreiben erneut für zahlreiche Eingaben in meiner Behörde. Mittlerweile war es April, und in der Impfreihenfolge waren nun diejenigen an der Reihe, die aufgrund von Vorerkrankungen besonders gefährdet waren. Die Angeschriebenen hegten den Verdacht einer unrechtmäßigen Datenweitergabe zwischen Krankenkassen und Ministerium.

Diesmal veranlasste das MS, dass die Krankenkassen ihren Versicherten ein entsprechendes Informationsschreiben schickten. Hierzu stellte das Ministerium den Krankenkassen einen Briefbogen zur Verfügung, welcher wieder den Briefkopf des MS und die Unterschrift der Ministerin trug. Bei einigen Angeschriebenen sorgten diese Briefe jedoch für erhebliche Verunsicherung. In etlichen Eingaben, die mich erreichten, wurde die Befürchtung geäußert, das MS habe möglicherweise Krankenkassendaten der Versicherten erhalten. Dieser Eindruck wurde dadurch bestärkt, dass die Krankenkasse als Absender meist nur in einem kleinen Feld aufgeführt war; teilweise war dieses Feld sogar leer. Auf meine Anfrage teilte mir das MS mit, zu keinem Zeitpunkt Daten der Krankenkassen erhalten zu haben und auch zu keinem Zeitpunkt Zugriff auf solche Daten gehabt zu haben. Vielmehr habe das MS den Krankenkassen nur ein Musterschreiben zur Verfügung gestellt.

Krankasse nicht deutlich als Absender zu erkennen

Meine Prüfung ergab, dass das Datenschutzrecht auch in diesem Fall eingehalten worden war. Eine Zugriffsmöglichkeit des MS auf Krankenkassendaten hatte zu keinem Zeitpunkt bestanden. Diejenigen, die sich mit einer Eingabe an mich gewandt hatten, wurden hierüber von mir informiert.

Wünschenswert wäre es in Zukunft, wenn im Rahmen von Informationskampagnen, bei denen Briefkopf und Unterschrift von einem anderen Haus stammen als vom tatsächlichen Absender, durch eine Erläuterung Missverständnisse und Verunsicherung vermieden würden.

J.2. Polizei

2.1 Prüfung der polizeilichen Leitstellen

In meinem 24. und 25. Tätigkeitsbericht hatte ich bereits über die Verarbeitung hochsensibler Daten in den kooperativen beziehungsweise eigenständigen Leitstellen der Polizei berichtet. Ich hatte im Rahmen meiner Prüfung festgestellt, dass in der entsprechenden Leitstellen-Software in Teilen personenbezogene Daten der Schutzstufe E meines Schutzstufenkonzeptes verarbeitet werden. Eine unsachgemäße Handhabung dieser Daten kann Gesundheit, Freiheit oder sogar das Leben der Betroffenen gefährden. Das Ziel meiner Prüfung war es, für einen bestmöglichen Schutz dieser Daten Sorge zu tragen.

Schutzstufenkonzept: https://t1p.de/schutzstufen

Wie berichtet, hatte die Polizeidirektion Oldenburg den Auftrag aus dem Niedersächsischen Ministerium für Inneres und Sport erhalten, eine Muster-Datenschutz-Folgenabschätzung (Muster-DSFA) für die betroffenen Leitstellen zu erstellen. So sollte nachvollzogen werden, ob die erforderlichen technisch-organisatorischen Maßnahmen zum Schutz der erhobenen Daten getroffen wurden. Ich hatte zunächst darauf bestanden, dass mir diese Muster-DSFA bis Ende Februar 2020 vorgelegt wird.

Erstellung einer DSFA gefordert – aber für neue Technik

Zwischenzeitlich habe ich aber darauf verzichtet, eine solche DSFA für ein auslaufendes Verfahren in den Leitstellen zu erhalten. Die Bemühungen der Polizei zur Implementierung einer vollkommen neuen Leistellentechnik und -software haben mittlerweile konkrete Formen angenommen. Ich gehe davon aus, dass die ersten polizeilichen Leitstellen noch im Jahr 2022 mit der neuen Technik und Software ausgestattet werden. Ich habe deshalb gefordert, mir eine ausführliche und aussagekräftige Muster-DSFA vor der ersten Inbetriebnahme der neuen Technik und Software vorzulegen. Die Zusicherung hierfür wurde mir gegeben. Die Inhalte und insbesondere die getroffenen technisch-organisatorischen Schutzmaßnahmen werde ich entsprechend bewerten.

Vertrag zur Auftragsverarbeitung erforderlich

Grundsätzlich wird die Einsatzleit-Software durch beauftragte IT-Unternehmen und deren Personal gewartet und betreut. Hierbei kommt es regelmäßig zu Fernwartungszugriffen über besonders gesicherte Leitungsverbindungen. Ein solcher Zugriff ermöglicht auch immer den Zugang zu den enthaltenen personenbezogenen Daten. Ich hatte zwischenzeitlich mehrfach gefordert, dass mir die Verantwortlichen der beteiligten Leitstellen entsprechende Verträge zur Auftragsverarbeitung vorlegen. Dieses ist mit einer Ausnahme auch geschehen.

Keine Nachweise zu Wartungszugriffen

Einer Polizeidirektion ist es bis zum Redaktionsschluss dieses Berichts nicht gelungen, mit dem Auftragnehmer einen Vertrag zur Auftragsverarbeitung abzuschließen. Ferner war es der Polizeidirektion nicht möglich, einen Nachweis darüber zu erbringen, ob und wann Fernwartungszugriffe erfolgt sind und ob sie einen Zugriff auf die enthaltenen personenbezogenen Daten beinhaltet haben. Ich habe diesen Umstand formell beanstandet und erwarte hierzu eine Stellungnahme durch das Niedersächsische Innenministerium.

Ich werde weiterhin darauf drängen, dass auch in dieser Leitstelle der Polizei eine rechtskonforme Datenverarbeitung umgesetzt wird.

2.2 Erhebliche Verzögerungen beim TKÜ-Zentrum im Nordverbund

Zuletzt habe ich in meinem Tätigkeitsbericht für das Berichtsjahr 2019 über die offenen Fragen für ein gemeinsames „Rechen- und Dienstleistungszentrum Telekommunikationsüberwachung der Polizei im Verbund der norddeutschen Küstenländer" (RDZ-TKÜ) berichtet. Dabei geht es um die Zusammenarbeit der Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein, durch die Synergieeffekte für die Länderpolizeien erzielt werden sollen. Die Planungen für dieses RDZ-TKÜ wurden bereits 2011 aufgenommen. Ziel des im August 2016 dafür in Kraft getretenen Staatsvertrages ist eine neue, gemeinschaftlich genutzte TKÜ-Anlage.

Die rechtlichen und technisch-organisatorischen Fragen, die meine Behörde gemeinsam mit den anderen betroffenen Aufsichtsbehörden zu diesem Projekt bis 2019 behandelt hat, entstanden im Rahmen von Beratungen für die Projektleitung. Die Umsetzung war hierbei mit Blick auf die sogenannte JI-Richtlinie, die in nationales Recht umzusetzen war, neu zu bewerten. Diese findet sich in Niedersachsen im zweiten Teil des Niedersächsischen Datenschutzgesetzes (NDSG) wieder. Daneben sind gleichberechtigt die zum Teil unterschiedlichen Bestimmungen der Landesdatenschutzgesetze der anderen beteiligen Länder zu berücksichtigen.

Lehren aus der Mängelliste der alten Anlage

Eine maßgebliche Rolle spielten dabei auch eine Reihe relevanter Anforderungen und Lehren, die sich aus der datenschutzrechtlichen Mängelliste der TKÜ-Anlage ergaben, die in Niedersachsen aktuell noch im Einsatz ist und bis zur Inbetriebnahme des neuen Verfahrens in Betrieb sein wird. Die daraus resultierenden beiden Stellungnahmen der Datenschutzaufsichtsbehörden der fünf beteiligten Länder im Jahr 2019 beinhalteten zahlreiche Details zu datenschutzrechtlichen Anforderungen, spezifischen Risiken und der Angemessenheit technisch-organisatorischer Maßnahmen. Darin waren unter anderem folgende zentrale Gesichtspunkte von besonderer Bedeutung:

Zentrale Anforderungen an eine TKÜ-Anlage

- Eine vollständige und pflegbare Datenschutz-Folgenabschätzung ist vor Aufnahme des Betriebes notwendig;
- Anforderungen der Auftragsverarbeitung müssen auch unter den Aspekten einer möglichen gemeinsamen Verantwortlichkeit für die gemeinsame Plattform des Verfahrens erfüllt werden;
- eine transparente und nachvollziehbare Methode zur Risikoidentifizierung, -bewertung und angemessenen -minimierung ist auszuwählen und durchzuführen;

- die Schutz- und Gewährleistungsziele sind vollständig abzubilden;
- eine hinreichend sichere Mandantentrennung insbesondere unter dem Gesichtspunkt einer mandantenübergreifenden Virtualisierung ist zu gewährleisten. Das heißt, trotz der funktionalen Nutzung gemeinsamer technischer Hard- und Software-Komponenten muss die Trennung der jeweiligen Daten und der funktional teils unterschiedlichen Anforderungen der Länderpolizeien sowie Dienststellen- und Organisationsebenen als Mandanten sichergestellt werden;
- es ist eine Möglichkeit zur Erweiterung, Deaktivierung und Reduzierung von Mandanten zu schaffen;
- Art und Umfang von Fernzugriffen sind zu definieren;
- Aspekte des Zugangs- und Zugriffsschutzes sind darzulegen;
- Umfang, Speicherdauer, Revisionssicherheit und Management von Protokolldaten sind zu klären;
- Malware-Schutz- und Backup-Lösungen sind auszugestalten.

Die Datenschutz-Folgenabschätzung muss mit einem methodisch einwandfreien Prozess durchgeführt werden. Dieser muss konsequent und ohne Abstriche beim Erfüllungsgrad der final festgelegten datenschutz-

rechtlichen Anforderungen umgesetzt werden. Andernfalls wären die polizeilichen TKÜ-Maßnahmen mit ihrer umfangreichen Eingriffstiefe in die Rechte und Freiheiten für die Betroffenen nicht tragbar und rechtlich unzulässig.

Die Hardware- und Software-Lösung für das Verfahren wird nicht durch die Polizei selbst, sondern durch einen IT-Dienstleister entwickelt und bereitgestellt. Der dafür erforderlichen Ausschreibung und Zuschlagserteilung im Jahr 2019 folgten 2020 und 2021 die Konkretisierungen und Implementierungen, jedoch noch keine Fertigstellung des Gesamtsystems, wie sie damals geplant war.

Geplanter Start um mehr als zwei Jahre verzögert

Zahlreiche Gründe für Verzögerung

Laut Staatsvertrag sollte der Wirkbetrieb schon mit Beginn des Jahres 2020 aufgenommen werden. Dieser Starttermin verzögerte sich erheblich durch die Ausschreibung, einen betrieblichen Standortwechsel und zusätzliche Wechselwirkungen sowie offenbar durch den hohen Komplexitätsgrad des Gesamtverfahrens. Zudem wurde bekannt, dass der IT-Dienstleister bei der Feinkonzeption und Implementierung in den Jahren 2020 und 2021 in Verzug geraten war. Seit 2021 gab es außerdem einen Wechsel in der Leitung und einem Teil des Fachpersonals der Projektgruppe sowie der projektinternen Datenschutzkoordination. Die zentrale Frage der Durchführung einer Datenschutz-Folgeabschätzung wurde durch die geschilderten Verzögerungen ebenfalls nicht zeitgerecht fertig.

Ein geplanter Beratungstermin mit der Datenschutzaufsicht zu offenen Umsetzungsfragen sollte im November 2021 stattfinden. Die dafür erforderliche Dokumentenlage zu einer Datenschutz-Folgenabschätzung konnte von der Projektleitung jedoch nicht zeitgerecht vorgelegt werden. Als neuer Beratungstermin wurde deshalb Anfang 2022 in Aussicht gestellt.

Ich sehe in den erheblichen Verzögerungen dieses Projektes – insbesondere wegen der noch nicht vorliegenden Datenschutz-Folgenabschätzung – ein erhebliches Problem. Die Abnahme des Gesamtverfahrens setzt die Lösung aller offenen Fragen und die vollständige Dokumentation voraus. Zugleich läuft der Betrieb des beanstandeten TKÜ-Altverfahrens weiter. Das ist jedoch angesichts der vor Jahren festgestellten Mängel, die nicht beseitigt worden sind, nicht hinnehmbar. Die Projektgruppe wurde von mir im Dezember 2021 erneut auf diese Konsequenzen hingewiesen.

2.3 Nutzung des Polizei-Messengers NIMes beanstandet

Über die flächendeckende Einführung des Niedersachsen-Messengers (NIMes) in der Niedersächsischen Polizei hatte ich zuletzt in meinem 26. Tätigkeitsbericht ausführlich berichtet. Das Prüfverfahren zur Nutzung von NIMes auf privaten Endgeräten der Beschäftigten der Polizei wurde mit einer Beanstandung abgeschlossen.

26. Tätigkeitsbericht: https://t1p.de/TB2020

Im Juni 2020 hatte legte mir das Niedersächsische Ministerium für Inneres und Sport (MI) eine Datenschutz-Folgenabschätzung (DSFA) zu NIMes vorgelegt. Dieser konnte ich entnehmen, dass bezüglich der Nutzung privater Endgeräte und der hierzu umgesetzten technisch-organisatorischen Schutzmaßnahmen erhebliche Sicherheitslücken. Als Folge dieser erkannten Lücken hatte ich unter anderem gefordert, ein sogenanntes Mobile Device Management (MDM) einzuführen, welches dem Verantwortlichen die komplette Kontrolle über die privaten Endgeräte ermöglicht hätte. Eine weitere Möglichkeit zum Schutz der verarbeiteten personenbezogenen Daten bis zur Schutzstufe D meines Schutzstufenkonzepts wäre aus meiner Sicht die ausschließliche Nutzung dienstlicher Endgeräte gewesen.

Schutzstufenkonzept der LfD: https://t1p.de/schutzstufen

Da weder ein MDM eingeführt noch auf die Nutzung privater Endgeräte verzichtet wurde, sprach ich gegenüber dem MI am 9. Februar 2021 eine Beanstandung gemäß § 57 Absatz 5 Niedersächsisches Datenschutzgesetz (NDSG) aus.

Innenministerium stellt Dienstgeräte in Aussicht

In seiner Stellungnahme vom 11. Mai 2021 stellte das MI in Aussicht, dass im Rahmen der Strategie „Mobile First“ der Polizei Niedersachsen eine Nutzbarkeit von mobilen Endgeräten für alle Einsatzszenarien geprüft werde. Überall dort, wo es möglich sei, solle zukünftig ein mobiles Endgerät dienstlich zur Verfügung gestellt werden. Es sei geplant, im Laufe des Jahres 2021 5.000 zusätzliche Smartphones und Tablets für die Polizistinnen und Polizisten anzuschaffen. NIMes werde als eine wesentliche Anwendung auf diesen Geräten bereitgestellt. Damit, so das MI weiter, erfolge sukzessive die Ablösung der Installationen auf privat genutzten Endgeräten. Die Zulassung der Nutzung von NIMes auf privaten Geräten sei von Anfang an als sichere und pragmatische Übergangslösung gedacht gewesen. Nicht nur vor dem Hintergrund dieser risikoorientierten Strategie seien aus datenschutzrechtlicher Sicht der Polizei Niedersachsen die verbleibenden Restrisiken vertretbar.

Die in der Stellungnahme enthaltene Bewertung des Restrisikos teile ich nicht. Mangels weitergehender gesetzlicher Befugnisse werde ich die weitere Entwicklung intensiv beobachten und mein Hauptaugenmerk auf den datenschutzkonformen Einsatz von NIMes auf den neu erworbenen dienstlichen Endgeräten richten.

Mit einer Kleinen Anfrage an die Landesregierung vom 14. Dezember 2021 erfragte die Fraktion Bündnis 90/Die Grünen unter anderem, wie viele Polizeibedienstete für die Nutzung von NIMes mit Dienstgeräten ausgestattet wurden bzw. werden.

Landtags-Drucksache 18/10499

Der Antwort des Niedersächsischem Ministeriums für Inneres und Sport vom 24. Januar 2022 ist zu entnehmen, dass im Jahr 2021 745 mobile dienstliche Endgeräte mit der Anwendung „NIMes“ in die Landespolizei ausgegeben wurden.

Von der zunächst in Aussicht gestellten Zahl von 5000 dienstlich angeschafften mobilen Endgeräten ist die Polizei somit noch sehr weit entfernt. Die Zahl der Nutzerinnen und Nutzer der Anwendung „NIMes“ ist inzwischen auf mehr als 21.500 angewachsen. Dies entspricht einem Anteil von ca. 80 Prozent der Beschäftigten und Studierenden in der Polizei Niedersachsen.

In Anbetracht meiner Forderung, die Anwendung nur auf dienstlichen Endgeräten zu nutzen, handelt es sich bei der oben geschilderten Umsetzung durch die schrittweise Ausgabe dienstlicher Endgeräte bislang nur um einen Tropfen auf den heißen Stein.

2.4 Mehr als 20 Jahre Erfahrungsaustauch mit den Datenschutzbeauftragten der Polizei

Bereits im Jahr 2000 wurde auf Wunsch der Datenschutzbeauftragten der Polizei ein regelmäßiger Erfahrungsaustausch mit meiner Behörde initiiert. Das so entstandene Netzwerk ist sehr effizient und für alle Beteiligten von Nutzen. Im Rahmen des Austausches werden datenschutzrechtliche Problemstellungen diskutiert um bestenfalls landeseinheitliche Lösungen zu finden. Hierbei liegt die Federführung nicht bei mir, vielmehr werde ich dabei als Beraterin tätig.

Teilnehmer und Teilnehmerinnen des Austausches sind die Datenschutzbeauftragten der Polizeidirektionen, des Landeskriminalamts Niedersachsen und der Polizeiakademie Niedersachsen. Pro Jahr finden mindestens zwei Treffen statt. In den Jahren 2018 und 2019 wurde der Austausch auf Grund der Umsetzung der sogenannten Datenschutz-Richtlinie im Bereich Justiz und Inneres (JI-Richtlinie) in den Zweiten Teil des Niedersächsischen Datenschutzgesetzes und das Niedersächsische Polizei- und Ordnungsbehördengesetz sogar stark intensiviert und monatlich abgehalten.

Ergebnisse des Austausches

Neben der Erörterung aktueller datenschutzrechtlicher Probleme im Arbeitsalltag der Polizei entstanden durch den Austausch auch mehrere Handlungsleitfäden, die im Berichtszeitraum aktualisiert oder fertig gestellt werden konnten:

Leitfäden tragen zur Vereinheitlichung bei

- Handlungsleitfaden für die Erfüllung von Auskunftsersuchen. Damit ist eine Vergleichbarkeit von Antworten auf Auskunftsersuchen möglich, selbst wenn diese aus verschiedenen Polizeidirektionen erteilt werden. Mit der Erstellung dieses Handlungsleitfadens wurde im Jahr 2019 begonnen. Bedingt durch hinzukommende elektronische Verarbeitungen in der Landespolizei ist dieser Leitfaden regelmäßig zu aktualisieren.
- Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten mit den notwendigen Inhalten auf Behördenebene.
- Vorgehensweise zur Erstellung einer Datenschutz-Folgenabschätzung einschließlich des erforderlichen Inhalts.
- Vorgehensweise bei der Prüfung polizeilicher Dateien und Protokollinhalte.

Blick in die Zukunft

Ich hoffe, dass dieser Erfahrungsaustausch weiterhin so erfolgreich durchgeführt werden kann und durch die hohe Sachkompetenz aller Beteiligten geprägt bleibt.

Neben tagesaktuellen datenschutzrechtlichen Problemstellungen wird im Jahr 2022 ein Hauptaugenmerk darauf gerichtet sein, die Einführung einer neuen polizeilichen Leitstellen-Software datenschutzrechtlich zu begleiten (siehe auch J.2.1, S. 109).

2.5 Prüfung des Schengener Informationssystems der zweiten Generation

Das Schengener Informationssystem der zweiten Generation (SIS II) ist ein Großinformationssystem zur vereinfachten Zusammenarbeit zwischen den nationalen Grenzkontroll-, Polizei-, Zoll-, Ausländer- und Justizbehörden im gesamten Schengen-Raum. Es ermöglicht den zuständigen Behörden der Schengener Mitgliedsstaaten Personen- und Sachfahndungen automatisiert auszuschreiben.

In den vergangenen Jahren sind die Ausschreibungen von Personenfahndungen zur verdeckten beziehungsweise gezielten Kontrolle in Strafsachen oder zur Gefahrenabwehr nach Artikel 36 SIS II-Beschluss[1] europaweit kontinuierlich angestiegen. Aus den Treffermeldungen einer Ausschreibung lassen sich umfassende Bewegungsbilder der betroffenen Person und ihrer Begleitpersonen generieren. Dies stellt einen intensiven Grundrechtseingriff dar.

Umfassende Bewegungsbilder sind möglich

1 Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation

Die Datenschutzaufsichtsbehörden haben daher beschlossen, durch eine koordinierte Prüfung ein Gesamtbild über die Nutzung dieses Instrumentes zu erhalten. Zugleich soll die Rechtmäßigkeit solcher Ausschreibungen in einer Stichprobe kontrolliert werden. Die Rechtsgrundlage für diese Prüfung lässt sich aus Artikel 1 SIS II-Gesetz[2], Artikel 60, Artikel 36 in Verbindung mit Artikel 37 SIS II-Beschluss ableiten.

Personenfahndungen durch niedersächsische Polizeibehörden

Die nationale Rechtsgrundlage für Ausschreibungen zur polizeilichen Kontrolle mit repressivem Fahndungszweck (Artikel 36 Absatz 2 Alternative 1 SIS II-Beschluss) ist § 163e der Strafprozessordnung (StPO).

Die länderspezifische Grundlage für Ausschreibungen zur polizeilichen Kontrolle mit präventivem Fahndungszweck (Artikel 36 Absatz 2 Alternative 2 SIS II-Beschluss) ergibt sich aus § 37 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes.

Daneben sind auch Ausschreibungen aus Anlass einer Führungsaufsicht gemäß § 463a StPO in Verbindung mit § 68 des Strafgesetzbuches möglich.

Vorläufiges Prüfergebnis

Zwei unrechtmäßige Speicherungen sofort gelöscht

Durch meine Behörde wurden die drei Polizeidirektionen mit dem zahlenmäßig höchsten Speicheraufkommen hinsichtlich ihrer Ausschreibungen zur Personenfahndung gemäß Artikel 36 Absatz 2 SIS II-Beschluss einer Vollprüfung unterzogen. Insgesamt konnten 53 gespeicherte Personenfahndungen, mithin circa 80 Prozent des prüfrelevanten Speicherbestandes der niedersächsischen Polizei, gesichtet werden.

Im Rahmen der Vor-Ort-Sichtung wurden zwei unrechtmäßige Speicherungen identifiziert. Diese wurden umgehend gelöscht.

Da die Auswertung vereinzelt ergänzende Rücksprachen mit den verantwortlichen Stellen erforderlich machte, dauerte die Prüfung zum Jahresende 2021 noch an. Das endgültige Prüfergebnis werde ich in meinem nächsten Tätigkeitsbericht vorstellen. Bei den zuständigen Polizeibehörden konnte ich jedoch grundsätzlich ein hohes Maß an Sorgfalt und Sensibilität im Zusammenhang mit den Ausschreibungen selbst sowie den Prüfungen feststellen.

2 Gesetz zum Schengener Informationssystem der zweiten Generation

2.6 Umsetzung „Bestandsdatenauskunft II“ in Niedersachsen

Mit seinem Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR 2618/13 – („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht (BVerfG) noch einmal verfassungsrechtliche Maßgaben für die Ausgestaltung des sogenannten manuellen Verfahrens zur Bestandsdatenauskunft aufgestellt. Dieses Auskunftsverfahren erfolgt jeweils einzelfallbezogen bilateral zwischen dem Telekommunikationsunternehmen und der hierfür berechtigten Stelle.

Zwar wurden im Rahmen der Verfassungsbeschwerden keine niedersächsischen Regelungen auf ihre Verfassungsmäßigkeit hin überprüft. Die in dem Beschluss enthaltenen Ausführungen lassen sich jedoch auf die hiesigen landesrechtlichen Vorschriften im Niedersächsischen Polizei- und Ordnungsbehördengesetz (NPOG) sowie im Niedersächsischen Verfassungsschutzgesetz (NVerfSchG) übertragen.

Leitsätze des Beschlusses: https://t1p.de/bverfg-bestand

Entscheidung des BVerfG

In seinem Beschluss stellte das BVerfG erneut heraus, dass sowohl die Übermittlung von Daten durch Anbieter von Telekommunikationsdiensten als auch der Abruf durch berechtigte Stellen jeweils einer Rechtsgrundlage bedürfen, die verhältnismäßig und normenklar ausgestaltet ist. Die Vorschriften zu Datenübermittlung und Abruf müssen laut Gericht die Verwendungszwecke hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden.[1]

Konkrete oder konkretisierende Gefahr

Dazu gehöre, dass für den Einsatz zur Gefahrenabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich im Einzelfall eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht vorliegen müssen. Zum Schutz von Rechtsgütern von erheblichem Gewicht kann auch das Vorliegen einer konkretisierenden Gefahr ausreichen. Nur ausnahmsweise bedarf es zum Schutz herausgehobener Rechtsgüter – wie etwa zur Verhütung terroristischer Straftaten – noch nicht einmal einer konkretisierenden Gefahr. Dann muss allerdings das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründen, dass sie solche Straftaten in überschaubarer Zukunft begehen wird.[2]

1 Siehe BVerfG, a. a. O., erster Leitsatz.
2 Siehe BVerfG, a. a. O., Rn. 148 ff.

Zeitliche Maßgabe erforderlich

Daraus ergibt sich, dass für die Rechtmäßigkeit einer Bestandsdatenauskunft in Bezug auf die Wahrscheinlichkeit, mit der eine Straftat erwartet wird, stets eine zeitliche Maßgabe gesetzlich vorgegeben sein muss.

Zudem muss die auf Verlangen der zuständigen Behörden durch den Telekommunikationsdienstleister erfolgende Zuordnung dynamischer IP-Adressen – also die numerische Kennung in Form einer normierten Ziffernfolge, über die jeder Computer innerhalb eines Netzwerks (etwa im Internet) eindeutig identifizierbar ist und die sich „dynamisch", also regelmäßig ändert – zu konkreten Personen dem Schutz und der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen.[3]

In Hinblick auf die genannten Aspekte wurden die Übermittlungsvorschrift des § 113 Telekommunikationsgesetz alter Fassung sowie eine Reihe damit korrespondierender Abrufregelungen im Fachrecht für unvereinbar mit dem Grundgesetz erklärt. Die bisherigen Vorschriften sollten zunächst weiter anwendbar bleiben, längstens jedoch bis zum 31. Dezember 2021.

Entschließung der Datenschutzkonferenz

DSK-Entschließung: https://t1p.de/Bestandsdaten

Mit ihrer Entschließung vom 25. November 2020 appellierte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) an die jeweiligen Bundes- und Landesgesetzgeber, die Vorgaben des BVerfG im Interesse der Rechtssicherheit zeitnah umzusetzen und die Frist des 31. Dezember 2021 nicht auszureizen.

Zudem äußerte die DSK, dass es geboten sei, nicht lediglich die unmittelbar von der Entscheidung betroffenen Regelungen anzupassen. Es müssten auch alle vergleichbaren Vorschriften, die Grundlage für Übermittlung und Abruf personenbezogener Daten sein können, mit Blick auf den Beschluss des BVerfG überprüft und gegebenenfalls verfassungskonform ausgestaltet werden. Dies betreffe im jeweiligen Landesrecht insbesondere Regelungen in den Polizei- und Verfassungsschutzgesetzen, die die Auskunftserteilung über Daten an die reine Aufgabenerfüllung der jeweiligen Stelle knüpfen. Derartige Regelungen würden die Gefahr einer unbegrenzten Datenverwendung bergen und seien daher unverhältnismäßig.[4] Datenabfragen dürften nicht länger aufgrund solch unbestimmter rechtlichen Grundlagen erfolgen.

3 Siehe BVerfG, a. a. O., vierter Leitsatz.
4 Vergleiche BVerfG, a. a. O., Rn. 154, 197.

Anhörung zu Niedersächsischen Gesetzentwürfen

In den Anfang 2021 vom Niedersächsischen Innenministerium im Rahmen der Verbandsbeteiligung vorgelegten Entwürfen zur Änderung des NPOG und des NVerfSchG waren noch keine etwaigen Änderungen zur Umsetzung der Entscheidung des BVerfG enthalten.

Zu den Gesetzentwürfen bezog ich im Rahmen öffentlicher Anhörungen vor den zuständigen Ausschüssen des Landtags im Februar 2021 Stellung (siehe auch G.1, S. 60). Dabei appellierte ich an den Niedersächsischen Gesetzgeber, die Regelungen des § 33 c NPOG sowie des § 20 NVerfSchG zeitnah anzupassen. Verbunden damit wies ich darauf hin, dass die derzeitige Ausgestaltung der genannten Vorschriften den Vorgaben des BVerfG nicht genügen und insofern als verfassungswidrig zu bewerten seien. So würde § 33 c NPOG nicht für alle Anwendungsvarianten zeitliche Maßgaben hinsichtlich der Wahrscheinlichkeit der Straftatenbegehung enthalten, die – wie oben geschildert – laut BVerfG erforderlich ist. Im Fall des § 20 NVerfSchG mangele es hingegen an der erforderlichen (normenklaren) Anknüpfung an den entsprechenden Gefahrentatbestand.

Keine Umsetzung in Niedersachsen

Bis zum Ablauf der durch das BVerfG vorgesehenen Frist zur Anwendbarkeit der betroffenen Regelungen, dem 31. Dezember 2021, wurden die hiesigen Vorschriften nicht verfassungskonform angepasst. Auf die Erforderlichkeit zur Anpassung der genannten Rechtsnormen werde ich im Rahmen der nächsten Gesetzesnovellierungen erneut hinweisen.

J.3. Justiz

3.1 Aufsichtsrechtliche Lücke – besondere Stellen im Justizsystem fehlen noch immer

Die Lücke bei der Datenschutzaufsicht im Justizbereich, auf die ich bereits in meinem 26. Tätigkeitsbericht hingewiesen habe, besteht weiterhin: „Besondere Stellen im Justizsystem", wie sie Erwägungsgrund (EG) 20 der Datenschutz-Grundverordnung (DS-GVO) vorsieht, sind bislang weder in Niedersachsen oder anderen Bundesländern noch auf Bundesebene eingerichtet.

Damit die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung unangetastet bleibt, sieht Artikel 55 Absatz 3 DS-GVO vor, dass Aufsichtsbehörden nicht für die Verarbeitung personenbezogener Daten durch Gerichte im Rahmen ihrer justiziellen Tätigkeit zuständig sein sollen. Mit der Aufsicht über diese Datenverarbeitungsvorgänge sollen stattdessen nach EG 20 der DS-GVO „besondere Stellen im Justizsystem" des Mitgliedsstaats betraut werden. Diese sollen insbesondere die Einhaltung der Verordnung sicherstellen, Richter und Staatsanwälte besser für die Pflichten aus der DS-GVO sensibilisieren und Beschwerden in Bezug auf derartige Datenverarbeitungsvorgänge bearbeiten. Diese Aufsichtsstellen im Justizsystem existieren derzeit in Deutschland nicht.

Andere EU-Staaten sind schon weiter

Erfahrungsberichte aus anderen europäischen Datenschutzaufsichtsbehörden haben jedoch gezeigt, dass andere Mitgliedsstaaten bereits nationale Regelungen zur Umsetzung des EG 20 DS-GVO geschaffen haben.

Nach meiner Auffassung fehlt es derzeit für die Einrichtung der besonderen Stellen im Justizsystem an einer gesetzlichen Grundlage. Eine solche müsste die Einrichtung beziehungsweise die Zusammensetzung und Befugnisse dieser Stellen regeln. Da die Erwägungsgründe allein der Auslegung von Rechtsnormen dienen, kommt EG 20 DS-GVO selbst als Rechtsgrundlage nicht in Betracht. Zudem stellt sich die Frage, in wessen Zuständigkeit die Schaffung einer Rechtsgrundlage fiele.

Austausch mit dem Justizministerium

Meine Behörde hat diesbezüglich mit dem Niedersächsischen Justizministerium (MJ) – wie im vorangegangenen Tätigkeitsbericht berichtet – den Austausch gesucht und betont, dass besonderen Stellen im Justizsystem dringend geschaffen werden müssen. Das Ergebnis der dortigen Prüfung liegt inzwischen vor.

Danach ist das MJ der Ansicht, die Zuständigkeit für die Einrichtung der besonderen Stellen im Justizsystem liege beim Bundesgesetzgeber. Dieser habe die Frage der (Nicht-)Einrichtung im Rahmen der konkurrierenden Gesetzgebung allerdings bereits abschließend geregelt, was für die Länder bindend sei. Durch die Regelung der Zuständigkeit der gerichtlichen Datenschutzbeauftragten in § 7 Absatz 1 Satz 2 BDSG bringe der Bundesgesetzgeber zum Ausdruck, dass kein justizinternes Kontrollgremium im Sinne des EG 20 DS-GVO zu etablieren sei.

Abweichende Einschätzungen

Ich stimme dem MJ insoweit zu, dass die Gesetzgebungskompetenz für die Errichtung der besonderen Stellen im Justizsystem der konkurrierenden Gesetzgebung des Bundes nach Artikel 74 Absatz 1 Nummer 1 Variante 3 und 4 GG unterfällt, da die Organisation des Gerichts betroffen ist. Nach Einschätzung meiner Behörde hat der Bundesgesetzgeber hinsichtlich der besonderen Stellen im Justizsystem jedoch bisher keine abschließende, für die Länder bindende Entscheidung getroffen.

Bisher keine abschließende Entscheidung vom Bund

Allein der Umstand, dass der Bundesgesetzgeber die Befugnisse des Datenschutzbeauftragten bei Gericht auf die Kontrolle administrativer gerichtlicher Tätigkeiten begrenzt, lässt noch nicht den Rückschluss zu, dass er damit ausdrücklich den Bereich der justiziellen Tätigkeit per se jeglicher Kontrolle entziehen wollte. Vielmehr wird durch die Regelung zum Ausdruck gebracht, dass eine Aufsicht durch einen Datenschutzbeauftragten über Gerichte im Rahmen ihrer justiziellen Tätigkeit nicht vorgesehen ist. Dies steht der Einrichtung der besonderen Stellen im Justizsystem jedoch nicht entgegen, da diese nicht zwangsläufig mit der Rolle des Datenschutzbeauftragten gleichzusetzen sind.

Lösungsansatz

Denkbar wäre die Einrichtung einer neben dem Datenschutzbeauftragten bestehenden justizinternen Stelle, deren ausschließliche Aufgabe darin besteht, die Einhaltung datenschutzrechtlicher Grundsätze während gerichtlicher Verfahren zu überprüfen.

Insgesamt erscheint eine bundeseinheitliche Regelung zweckmäßig und sinnvoll. In Anbetracht dessen, dass durch das Handeln dieser besonderen Stellen im Justizsystem die grundrechtlich geschützte richterliche Unabhängigkeit berührt werden könnte, ist eine zentrale, für alle Länder geltende Regelung gegenüber einer länderspezifischen Regelung vorzugswürdig.

Zentrale Lösung wäre vorzuswürdig

Weiteres Vorgehen

Die Datenschutzaufsichtsbehörden haben den Handlungsbedarf in dieser Angelegenheit erkannt. Bislang ist noch nicht absehbar, wann sich etwa der Europäische Datenschutzausschuss (EDSA) auf europäischer Ebene mit dem Thema befassen wird. Daher wird derzeit in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern angestrebt, mit einem gemeinsamen Papier die zuständigen innerdeutschen Akteure auf das Problem aufmerksam zu machen. Zugleich ist beabsichtigt, in dem Papier dazu anzuregen, die bestehende Problematik mit einer bundeseinheitlichen Regelung zu lösen.

3.2 Einzelfall versus Erlass des Justizministeriums – Aufsicht über Staatsanwaltschaften

Siehe Tätigkeitsbericht 2020, Kapitel J.3.3.: https://t1p.de/TB2020

Im Fall einer Datenverarbeitung einer Staatsanwaltschaft hat sich meine Behörde – entgegen der Erlasslage des Niedersächsischen Justizministeriums (MJ) – zuständig für die Aufsicht erachtet. Zu diesem Thema habe ich bereits im Allgemeinen im vorangegangenen Tätigkeitsbericht berichtet.

Ich hatte eine Beschwerde wegen der Übermittlung einer Anklageschrift durch eine Staatsanwaltschaft an die Fahrerlaubnisbehörde eines Landkreises erhalten. In diesem Fall erachtete ich meine Behörde hinsichtlich der Aufsicht über die Staatsanwaltschaft – entgegen deren Einschätzung – für zuständig. Das wurde auch gegenüber den Beschwerdeführer entsprechend vertreten.

Die Staatsanwaltschaft hatte sich zuvor unter Berufung auf den Erlass des MJ vom 9. Juli 2020, Aktenzeichen 9510/1 – 402. 353 (SH 3), geweigert, gegenüber meiner Behörde eine Stellungnahme abzugeben. Streitgegenständlich war hier die Norm des § 57 Absatz 3 des Niedersächsischen Datenschutzgesetzes (NDSG). Gemäß dieser Regelung ist die Aufsicht meiner Behörde über die Erhebung personenbezogener Daten durch Strafverfolgungsbehörden bei der Ermittlung, Aufdeckung oder Verfolgung von Straftaten erst nach Abschluss des Strafverfahrens zulässig. Diese Ausschlussnorm kam hier jedoch nicht zur Anwendung. Der Abschluss des Strafverfahrens lag vor, es war mit Ablehnung der Eröffnung des Hauptverfahrens gegenüber dem Betroffenen durch das zuständige Amtsgericht abgeschlossen worden.

Keine Veränderung der Akte durch datenschutzrechtliche Prüfung

Gemäß dem genannten Erlass des MJ würde ein Verfahrensabschluss im Sinne des § 57 Absatz 3 NDSG hingegen stets erst mit Eintritt der Verfolgungsverjährung eintreten. Danach wäre erst ab diesem Zeitpunkt die Aufsicht durch meine Behörde gegeben.

Es lagen jedoch keine Gründe vor, die in diesem Fall einen derartig späten Zeitpunkt für den Beginn meiner Zuständigkeit rechtfertigen würden. Etwaige dagegensprechende Befürchtungen trafen nicht zu. So wurde hier womöglich die Gefahr gesehen, dass Akteninhalte durch Aufsichtsmaßnahmen

meinerseits verändert werden könnten, bevor ausgeschlossen werden kann, dass diese noch einmal für die Strafverfolgung – etwa im Rahmen einer Wiederaufnahme – benötigt werden. Dem lässt sich entgegenhalten, dass bezogen auf diesen Fall mit der datenschutzrechtlichen Prüfung keinerlei Veränderung der Akten bezweckt oder zu erwarten war. Vor Gericht stünden im Fall einer etwaigen zukünftigen Wiederaufnahme des Strafverfahrens immer die unveränderten Akten zur Verfügung. Hier ging es vielmehr um die Überprüfung der Rechtmäßigkeit einer Datenübermittlung von einer Staatsanwaltschaft an eine andere öffentliche Stelle.

Ich teilte der betreffenden Staatsanwaltschaft und dem MJ mit, dass ich im vorliegenden Fall die datenschutzrechtliche Aufsicht über die Staatsanwaltschaft durch meine Behörde nach erfolgter Prüfung als zulässig erachtet habe. Eine Reaktion des MJ und der Staatsanwaltschaft auf diese Mitteilung blieb aus. Es ist nicht auszuschließen, dass sich die jeweiligen Auffassungen der Staatsanwaltschaften und des MJ einerseits sowie meiner Behörde andererseits bei zukünftigen Fällen erneut gegenüberstehen werden.

J.4. Kommunen und Landesverwaltung

4.1 Prüfung zum Einsatz von Windows 10 in der niedersächsischen Landesverwaltung

Wie im vorausgegangenen Tätigkeitsbericht angekündigt, habe ich den Einsatz des Betriebssystems Windows 10 mit Blick auf die Übermittlung personenbezogener Telemetriedaten an Microsoft in fünf Behörden der niedersächsischen Landesverwaltung geprüft. Die Prüfung verlief konstruktiv. Einige der identifizierten Mängel wurden von den Verantwortlichen bereits nach den ersten Gesprächen noch vor Übermittlung des Prüfungsberichtes behoben.

Neben Enterprise-Edition und Telemetriestufe „security" weitere Maßnahmen erforderlich

Zum Zeitpunkt der Prüfung setzten vier der fünf geprüften Behörden die „Enterprise"-Edition von Windows 10 mit der Telemetriestufe „security" ein und konnten durch weitere technische Maßnahmen die Übermittlung von personenbezogenen Telemetriedaten an Microsoft unterbinden. Lediglich eine Behörde verwendete noch die „Professional"-Edition und konnte nicht nachweisen, dass keine Telemetriedaten übertragen wurden. Die Behörde sagte jedoch einen Wechsel auf die „Enterprise"-Edition zu.

Verbesserungsbedarf bei Wirksamkeitskontrolle

Regelmäßige Überprüfung der getroffenen Maßnahmen nötig

Mit der Veröffentlichung neuer Versionen oder Release-Stände können sich das Kommunikationsverhalten und die Konfigurationsmöglichkeiten von Windows 10 ändern. Daher müssen Verantwortliche regelmäßig den Datenverkehr zu den Microsoft-Servern darauf prüfen, inwieweit die bislang ergriffenen Schutzmaßnahmen noch wirksam sind. Derartige Kontrollmaßnahmen wurden jedoch in keiner der geprüften Behörden durchgeführt. Daher forderte ich die Verantwortlichen auf, ein entsprechendes Netzwerk-Monitoring zu etablieren.

Im Jahr 2022 werde ich in zwei Fällen Nachprüfungen zu den zugesagten Maßnahmen durchführen und die Prüfung darüber hinaus in den kommunalen Bereich ausweiten.

4.2 Unterstützung der Projekte zum Onlinezugangsgesetz

Die Verwaltungsdigitalisierung kann nur mit angemessenem Datenschutz rechtskonform umgesetzt werden. Daher berate ich die Gremien des Programms „Digitale Verwaltung Niedersachsen" und stehe mit dem Niedersächsischen Sozialministerium zur Umsetzung des Onlinezugangsgesetzes (OZG) in Kontakt.

Schwerbehindertenausweis als „Muster"

Das Niedersächsische Ministerium für Soziales, Gesundheit und Gleichstellung (MS) ist federführend für die Digitalisierung der Online-Leistungen im Gesundheitsbereich zuständig. Seit 2021 befinde ich mich im Austausch mit dem MS über die Umsetzung der Online-Leistung „Schwerbehindertenausweis"; die Erkenntnisse daraus sollen auch bei der Umsetzung weiterer Gesundheitsleistungen verwendet werden. Insbesondere berate ich das Ministerium zur Datenschutzfolgenabschätzung gem. Art. 35 DS-GVO.

Mitarbeit in den Gremien der DSK

Einer-für-Alle-Prinzip bringt datenschutzrechtliche Fragen mit sich

Der Arbeitskreis „Verwaltung" der Datenschutzkonferenz (DSK) unterstützt die Umsetzung des OZG und insbesondere des „Einer-für-Alle"-Prinzips. Das Prinzip fordert, dass jedes Land die Verwaltungsleistungen so digitalisiert, dass andere Länder sie auch nutzen können und den Online-Prozess nicht nochmal selbst entwickeln müssen. Diese bislang eher unübliche Form der Zusammenarbeit zwischen Bundesländern und Kommunen bei digitalisierten Verwaltungsleistungen erfordert zusätzliche, klare Regelungen. Dabei stellen sich insbesondere Fragen der datenschutzrechtlichen Verantwortlichkeit und der Rechtsgrundlagen der Verarbeitung in jedem einzelnen Verarbeitungsschritt. Es wäre für einen Bürger oder eine Bürgerin nicht zumutbar, sich beim Versuch, Rechte als betroffene Person geltend zu machen, in einem ungeklärten Durcheinander von Zuständigkeiten zu verlieren.

Die DS-GVO definiert klare Verantwortlichkeiten von der Antragstellung bis zum Bescheid. Daher steht der Arbeitskreis Verwaltung unter meiner Beteiligung insbesondere in Kontakt mit dem Bundesministerium des Inneren und für Heimat und der Föderalen IT-Kooperation (FITKO). Ziel der Zusammenarbeit ist ein einheitliches Verständnis für die datenschutzrechtlichen Anforderungen an die beteiligten Leistungserbringer in jedem Einzelschritt und die einheitliche Umsetzung in Ländern und Kommunen.

4.3 Einsatz von „Cisco Webex Meetings“ in der Landesverwaltung

Die Corona-Pandemie hat auch im öffentlichen Bereich zu einem gesteigerten Bedarf an Videokonferenzlösungen geführt. Aufgrund einer Anfrage des Niedersächsischen Ministeriums für Inneres und Sport habe ich mich mit der Frage befasst, inwiefern ein datenschutzkonformer Einsatz der cloud-basierten Videokonferenzlösung „Cisco Webex Meetings“ möglich ist.

Zuvor hatten die Datenschutzaufsichtsbehörden mehrere Dokumente zum Einsatz von Videokonferenzsystemen veröffentlicht.[1] Zwei wesentliche Problemfelder waren die Auftragsverarbeitungsvereinbarung mit dem Anbieter des Videokonferenzsystems und die Übermittlung personenbezogener Daten in sogenannte Drittländer.

Die vom Innenministerium vorgelegte Vereinbarung zur Auftragsverarbeitung erfüllte nicht vollständig die Anforderungen des Art. 28 Abs. 3 DS-GVO. Zu den Defiziten der Vereinbarung, der im Wesentlichen ein Standardmuster der Firma Cisco zugrunde lag, zählten unter anderem die folgenden:

AV-Vereinbarung entspricht nicht Anforderungen der DS-GVO

- Es war nicht auszuschließen, dass der Anbieter Cisco personenbezogene Daten neben der Verarbeitung im Auftrag auch zu eigenen Zwecken verarbeitet; hierfür bedarf es einer Rechtsgrundlage; dieses Vorgehen ist über das Konstrukt der Auftragsverarbeitung nicht zu legitimieren.
- Die Verarbeitung personenbezogener Daten nach Weisung wurde unter Vorbehalt der Konformität mit Gesetzen (und zwar auch solcher der Drittländer) gestellt. Das kann in letzter Konsequenz zur Folge haben, dass der Auftragsverarbeiter personenbezogene Daten nach Maßgabe des Rechts von Ländern verarbeitet, deren Datenschutzniveau nicht dem europäischen entspricht.
- Es lagen Einschränkungen oder zumindest missverständliche Formulierungen zu den Betroffenenrechten vor.
- Die Möglichkeit des Verantwortlichen zum Einspruch gegen den Einsatz eines Unterauftragnehmers wurde an die Nennung eines wichtigen Grundes geknüpft und damit in unzulässiger Weise eingeschränkt.

1 Unter anderem in der Orientierungshilfe der DSK vom 23.10.2020 (https://t1p.de/oh-vk-systeme) nebst Checkliste vom 11.11.2020 (https://t1p.de/ckeck-vk-systeme) und in den Fragen und Antworten zu Videokonferenzsystemen aus meinem Haus, Stand August 2020: https://t1p.de/ds-videokonferenz

Aus den vorgelegten Vertragsunterlagen ist ersichtlich, dass während des Einsatzes des Videokonferenzsystems personenbezogene Daten verschiedener Datenkategorien insbesondere an Server-Standorte in den USA übermittelt werden. Zur Absicherung der Datenübermittlung nach Art. 46 DS-GVO wurden die Standardvertragsklauseln gemäß Kommissionsbeschluss 2010/87/EU vom 5. Februar 2010 verwendet. In Bezug auf die mit dem Drittlandtransfer verbundenen Herausforderungen wird auf Kapitel D.2 der Klauseln verwiesen. Es wurden insbesondere keine zusätzlichen Maßnahmen zur Sicherstellung eines dem in der EU im Wesentlichen gleichwertigen Schutzniveaus dargelegt.

Keine ausreichende Rechtsgrundlage für Drittlandtransfer

Aufgrund dieser erheblichen rechtlichen Unsicherheiten beim Einsatz von Cisco Webex in dem mir vorgestellten Betriebsmodell stehe ich in Kontakt mit dem Niedersächsischen Innenministerium bezüglich möglicher Alternativlösungen, die die datenschutzrechtlichen Anforderungen erfüllen.

4.4 Fortführung der Kommunalprüfung

Nachdem im Rahmen der ersten Kommunalprüfung in den Jahren 2018/2019 einige datenschutzrechtliche Defizite bei den geprüften Kommunen festgestellt wurden, habe die Prüfung im Berichtszeitraum auf weitere niedersächsische Kommunen ausgeweitet.

Im Dezember 2021 habe ich 50 weiteren Kommunen, die nicht Teil der ersten Prüfung waren, meine Fragen übersandt. Da die Ergebnisse der ersten Kommunalprüfung Probleme bei der Umsetzung allgemeiner Pflichten der DS-GVO aufzeigten, werden ausgewählte Punkte in der Prüfung wieder aufgegriffen. Der zweite Teil der Prüfung basiert auf mir vorgetragenen wiederkehrenden Sachverhalten von Beschwerden.

Prüfung und dann?

Zum Ende des Berichtszeitraums lagen noch keine Antworten der geprüften Kommunen vor. Sobald ich im Laufe des Jahres 2022 Erkenntnisse gewonnen habe, werde ich auf dieser Grundlage weitere Hilfestellungen veröffentlichen, um die Kommunen bei der Umsetzung ihrer datenschutzrechtlichen Verpflichtungen zu unterstützen.

4.5 Wahlwerbung und Meldedaten

Im Vorfeld der Kommunalwahl und der Bundestagswahl 2021 haben die Parteien Wahlwerbung versandt. Es wurde auch die Möglichkeit genutzt, bestimmte Wählergruppen persönlich anzuschreiben. In diesem Zusammenhang haben sich Bürgerinnen und Bürger bei mir erkundigt, ob die Einwohnermeldeämter den Parteien Meldedaten für Wahlwerbung übermitteln dürfen.

Grundlage für die Führung des Melderegister ist das Bundesmeldegesetz (BMG). Dort ist auch geregelt, in welchen Fällen das Einwohnermeldeamt personenbezogene Daten aus dem Melderegister an andere Stellen übermitteln darf. Weitere ergänzende Regelungen enthält das Niedersächsische Ausführungsgesetz zum Bundesmeldegesetz (Nds. AG BMG). Die Übermittlung von Meldedaten in Zusammenhang mit Wahlen und Abstimmungen ist unter den in § 50 Abs. 1 BMG genannten Voraussetzungen möglich:

- Die Auskunft darf nur für nach dem Lebensalter bestimmte Gruppen von Wahlberechtigten erteilt werden. Die Eingrenzung der Gruppe (z. B. Jungwähler) obliegt den Anfrageberechtigten.
- Die Auskunft umfasst Familienname, Vorname, Doktorgrad und Anschrift. Die Übermittlung des Geburtsdatums ist nicht zulässig.
- Die übermittelten Daten dürfen nur zur Wahlwerbung verwendet werden und sind spätestens einen Monat nach der Wahl zu löschen oder zu vernichten.
- Eine Nutzung der personenbezogenen Daten für andere Zwecke, z. B. zur Mitgliederwerbung, ist unzulässig.
- Eine Einwilligung der Wahlberechtigten ist nicht erforderlich. Die Übermittlung kann bereits bis zu sechs Monate vor der Wahl erfolgen.

Keine Nutzung für andere Zwecke erlaubt

Widerspruch ist möglich

Es besteht die Möglichkeit der Datenweitergabe für Wahlwerbung zu widersprechen (§ 50 Abs. 5 BMG). Auf diese Möglichkeit weist die Meldebehörde bei der Anmeldung des Wohnsitzes und einmal jährlich durch öffentliche Bekanntmachung hin. Der Widerspruch kann der Kommune formlos mitgeteilt werden. Häufig liegen in Rathäusern und Bürgerämtern auch bereits vorgefertigte Widerspruchsvordrucke aus, auf denen angekreuzt werden kann, welchen Datenweitergaben widersprochen wird.

Vordrucke für Widerspruch in Bürgerämtern

Die Meldebehörden haben sicherzustellen, dass eingegangene Widersprüche bei der Datenübermittlung berücksichtigt werden. Hier obliegt den Kommunen eine besondere Verantwortung. Verstöße durch Meldebehörden oder Parteien konnte ich im Jahr 2021 nicht feststellen.

4.6 Zensus 2022 – Niedersachsen ist datenschutzkonform aufgestellt

Die Vorbereitungen zum Zensus 2022 in Niedersachsen wurden von mir eng begleitet. Der Zensus 2022 ist wichtig und sinnvoll; datenschutzrechtliche Bedenken bestehen keine.

Erster Zensus seit elf Jahren

Bereits im Berichtsjahr 2019 hatte ich über die Vorarbeiten des Bundesgesetzgebers zu der lange geplanten, alle zehn Jahre stattfindenden Volkszählung – dem sogenannten Zensus – informiert. Zu diesem Zeitpunkt hatte der Bundesgesetzgeber im Zensusgesetz die Vorgaben des Bundesverfassungsgerichts aus dem Volkszählungsurteil umgesetzt. Am Ende des Berichtsjahrs 2021, stand der Zensus nun kurz bevor. Zwischenzeitlich hatte sich die Befragung um ein Jahr verschoben. Vor dem Hintergrund der allgemeinen Pandemielage hatte der Bundestag den Zensus durch Änderung des Zensusgesetzes auf das Jahr 2022 verlegt. Der sogenannte Zensusstichtag ist nun der 15. Mai 2022. Damit findet nun erstmals seit elf Jahren wieder ein Zensus in Deutschland statt.

Gesetzlicher Ausschluss der Betroffenenrechte in Einklang mit der DS-GVO

Die Verschiebung des Zensus auf 2022 machte zwischenzeitlich auch im Entwurf des Niedersächsischen Ausführungsgesetzes Anpassungen erforderlich. Daher wurde mir 2021 der Entwurf des Niedersächsischen Ausführungsgesetzes zum Zensusgesetz 2022 erneut zur Prüfung vorgelegt. Gegen den darin vorgesehenen Ausschluss der Betroffenenrechte beim bevorstehenden Zensus bestehen keine datenschutzrechtlichen Bedenken.

Kein Recht auf Auskunft, Berichtigung oder Widerspruch

Die DS-GVO sieht in Art. 89 Abs. 2 ausdrücklich die Möglichkeit eines Ausschlusses der Betroffenenrechte nach Art. 15, 16, 18 und 21 DS-GVO vor, wenn die Datenverarbeitung zu statistischen Zwecken erfolgt und die dort aufgeführten datenschutzrechtlichen Garantien gewahrt sind. Diese Ausschlussmöglichkeit betrifft also neben dem Auskunftsrecht des Art. 15 DS-GVO auch das Recht auf Berichtigung (Art. 16 DS-GVO), auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) und das Widerspruchsrecht des Art. 21 DS-GVO.

§ 6 Niedersächsisches Ausführungsgesetz zum Zensusgesetz 2022 gibt den Wortlaut des Art. 89 Abs. 2 DS-GVO exakt wieder und wird zudem in Gliederungsnummer 8 der Verwaltungsvorschrift zum Niedersächsischen Ausführungsgesetz zum Zensusgesetz 2022 (VV-Nds. AG ZensG 2022) näher konkretisiert. Durch eine Gewährung der genannten Betroffenenrechte während der laufenden Erhebung würde der auf anonyme Statistiken zielende Zensus stark beeinträchtigt oder sogar unmöglich gemacht werden. Entscheidend ist hierbei, dass es dieser Betroffenenrechte bei einem Massenverfahren, das letztlich auf die Erstellung anonymer Statistiken abzielt, grundsätzlich nicht bedarf, sofern der nationale Gesetzgeber diese von der DS-GVO geschaffene Möglichkeit aufgreift und die geforderten Garantien gewährt. Beide Voraussetzungen sind in Niedersachsen gegeben. Es bestehen daher keine datenschutzrechtlichen Bedenken gegen den Ausschluss der Betroffenenrechte.

Enge Begleitung der Zensus-Vorbereitungen

Neben der Begleitung des dargestellten Gesetzesentwurfs war ich im Berichtsjahr in regelmäßigen Terminen mit dem Niedersächsischen Innenministerium und dem Niedersächsischen Landesamt für Statistik (LSN) in die Vorbereitungen der Behörden zum Zensus 2022 eingebunden. Meine Beratung bezog sich sowohl auf die Datenschutzfolgenabschätzung des LSN als auch auf Maßnahmen der Abschottung (dazu unten mehr) der kommunalen Erhebungsstellen von der übrigen Kommunalverwaltung.

Vorbefragung zur Gebäude- und Wohnungszählung

Faktisch hat die Durchführung des aktuellen Zensus bereits im Jahr 2021 begonnen – und zwar mit der sogenannten Vorbefragung zur Gebäude- und Wohnungszählung. Gemäß § 6 Abs. 1 Bundesstatistikgesetz kann der Kreis der zu Befragenden durch eine Vorbefragung geklärt werden, sofern es sich um eine durch Rechtsvorschrift angeordnete Bundesstatistik handelt. Eine solche Bundesstatistik ist auf der Grundlage des Zensusgesetz 2022 des Bundes gegeben. Mit der Vorbefragung wird beispielsweise geklärt, ob die angeschriebene Person tatsächlich Eigentümer oder Eigentümerin der jeweiligen Immobilie und daher auskunftspflichtig ist. Da mich zu dieser Vorbefragung zur Gebäude- und Wohnungszählung mehrere Beratungsanfragen von Angeschriebenen erreichten, habe ich den Anfragenden jeweils die Rechtslage dargestellt und konnte insbesondere mitteilen, dass die Voraussetzungen des Bundesstatistikgesetzes für die Durchführung einer Vorbefragung erfüllt sind.

Rechtliche Eckpunkte des Zensus 2022

Der Zensus 2022 wird nicht als Totalerhebung (welche eine Befragung sämtlicher Bürgerinnen und Bürger wäre) durchgeführt. Stattdessen beruht er – wie bereits im Jahr 2011 – teilweise auf Erhebungen aus den Melderegistern der Kommunen. Nur noch ergänzend erfolgt auf Stichprobenbasis die Haushaltsbefragung. Zusätzlich werden die Eigentümerinnen und Eigentümer von Gebäuden und Wohnungen befragt. Außerdem erfolgen Befragungen in Wohnheimen und Gemeinschaftsunterkünften.

Daten dienen ausschließlich statistischen Zwecken

Es ist gesetzlich geregelt, dass die erhobenen Angaben nur statistischen Zwecken dienen. Daher ist es ausgeschlossen, dass die Daten für Einzelfälle wie beispielsweise eine Korrektur des Melderegisters verwendet werden. Gemäß § 23 Zensusgesetz 2022 besteht eine gesetzliche Auskunftspflicht. Durch zahlreiche gesetzlich vorgeschriebene Vorkehrungen ist die Vertraulichkeit der erhobenen Angaben gesichert. Insbesondere sind die in den Erhebungsstellen tätigen Personen gesetzlich zur Geheimhaltung verpflichtet. Die Erhebungsbeauftragten haben gemäß § 20 Abs. 5 Zensusgesetz 2022 die Unterlagen unverzüglich der Erhebungsstelle auszuhändigen. Gemäß § 19 Abs. 2 Zensusgesetz 2022 sind die Erhebungsstellen räumlich, organisatorisch und personell von den übrigen Verwaltungsbereichen abgeschottet. Auf diese Weise ist die Zweckbindung zu statistischen Zwecken gesichert.

Auftrag an Dienstleister ist datenschutzkonform

Es ist mir wichtig, auf einen zentralen Aspekt ausdrücklich hinzuweisen. Die DS-GVO erlaubt, dass der datenschutzrechtlich Verantwortliche externe Dienstleister für die Datenverarbeitung beauftragt. Die DS-GVO verwendet hierfür den Fachbegriff „Auftragsverarbeitung". Das bedeutet, dass der sogenannte Auftragsverarbeitungsnehmer, d. h., der externe Dienstleister, nur unter Aufsicht und gemäß den Weisungen des Verantwortlichen die Daten für diesen verarbeitet. Rechtlich handelt es sich bei einer Zusammenarbeit mit dem Dienstleister nicht um eine Datenübermittlung, die eine gesonderten Übermittlungsregelung erfordern würde. Vielmehr wird jede Verarbeitung durch den Dienstleister dem Verantwortlichen zugerechnet, beispielsweise dem LSN.

Beim Zensus 2022 macht das LSN von dieser Möglichkeit Gebrauch. Gegen den Einsatz von solchen unterstützenden Dienstleistern etwa für die Bereiche IT, Beleg-Einlesung, Telefonie (Hotline) und Druck bestehen ausdrücklich keine datenschutzrechtlichen Bedenken. Ich betone nochmals, dass bei Einbeziehung solcher unterstützenden Dienstleister keine Übermittlung an Dritte im Rechtssinne erfolgt. Rechtlich Handelnder ist allein der Verantwortliche, in diesem Fall also das LSN.

4.7 Keine Warnung vor der Tätigkeit von Einzelpersonen ohne Rechtsgrundlage

Oftmals gut gemeint warnen öffentliche Stellen gelegentlich vor Tätigkeiten durch einzelne Gewerbetreibende und nennen dabei explizit Namen. Dabei wird mitunter außer Acht gelassen, dass hierfür eine Rechtsgrundlage erforderlich ist.

So erreichte mich die Beschwerde eines eingetragenen Kaufmannes (e. K.) gegen eine Landesoberbehörde, die unter Nennung des Firmennamens auf ihrer Webseite vor dessen Tätigkeit warnte.

Firmenname kann personenbezogenes Datum sein

Zunächst stellte sich mir die Frage, ob der Firmenname eines e. K. überhaupt ein personenbezogenes Datum ist. Nach Rechtsprechung des Europäischen Gerichtshofs können in Einzelfällen selbst Daten einer juristischen Person personenbezogene Daten sein, wenn eine enge Verknüpfung mit der dahinterstehenden natürlichen Person besteht, so zum Beispiel bei einer Ein-Mann-GmbH. Da es sich bei einem e. K. nicht um eine juristische Person handelt, sondern eine Personalunion zwischen dem Gewerbetreibenden und der Privatperson besteht, handelt es sich bei dessen Firmennamen um ein personenbezogenes Datum.

Für die Veröffentlichung des Namens eines e. K. durch eine Behörde ist daher eine Rechtsgrundlage erforderlich. Eine solche existiert nicht, sodass die Veröffentlichung des Firmennamens im vorliegenden Fall rechtswidrig war. Die verantwortliche Landesoberbehörde wurde daher von mir in Bezug auf eine mögliche Anweisung zur Entfernung des Namens von der Webseite angehört. Sie entfernte in der Folge den Namen. Wegen des damit nun in der Vergangenheit liegenden Verstoßes habe ich die Landesoberbehörde verwarnt.

Verwarnungen gegen Behörde und Innungsverband

In einer ähnlichen Konstellation warnte ein Landesinnungsverband mit einem Rundschreiben vor den Tätigkeiten bestimmter, namentlich genannter Handwerker. Dieses Rundschreiben wurde an zahlreiche Friedhofsträger verschickt. Eine Rechtsgrundlage für dieses Vorgehen gab es nicht, sodass ich auch eine Verwarnung gegenüber dem Landesinnungsverband ausgesprochen habe.

J.5. Schule und Hochschule

5.1 Monitoring an berufsbildenden Schulen

Der Schulträger einer berufsbildenden Schule (BBS) bat mich um eine datenschutzrechtliche Bewertung zur Zulässigkeit der Verarbeitung personenbezogener Daten von Schülerinnen und Schülern für ein Monitoring. Im Rahmen des Monitorings wollen mehrere Schulträger einer Region zusammenarbeiten und auf Basis einer gemeinsamen Datengrundlage ein bedarfsgerechtes, ausgewogenes und ortsnahes Beschulungsangebot bereitstellen. Dafür soll erhoben werden, wie viele Schülerinnen und Schüler weite Pendelwege auf sich nehmen, um von ihrem Wohnort bzw. von ihrer Ausbildungsstätte zur Schule zu kommen.

Weite Anreisewege sollen vermieden werden

Die Schulen im Zuständigkeitsbereich der beteiligten Schulträger sollen u. a. die Anschrift, Klassenstufe, Ausbildungsberufe sowie die Anschriften der Ausbildungsbetriebe von Schülerinnen und Schülern an die Schulträger übermitteln. Auf Basis dieser Daten soll von den Schulträgern geprüft werden, ob vorhandene Bildungszweige an den BBS verändert oder neu eingerichtet werden könnten, um weite Anreisen für Schülerinnen und Schüler zu vermeiden.

Voraussetzungen für die Datenverarbeitung

Da es sich bei diesen Daten um personenbezogene Daten handelt, ist bereits für ihre Übermittlung von der Schule an den jeweiligen Schulträger eine Rechtsgrundlage erforderlich. Die Verarbeitung personenbezogener Daten durch die Schulen ist in § 31 Niedersächsisches Schulgesetz abschließend geregelt. Dort finden sich auch Regelungen, in welchen Fällen personenbezogene Daten an den Schulträger übermittelt werden dürfen.

Stadtteil ist ausreichend – keine Erhebung der Adresse nötig

Die Übermittlung der in Rede stehenden Daten sind von den bestehenden Regelungen für den Zweck des Monitorings jedoch nicht abgedeckt. Zudem wäre eine Verarbeitung personenbezogener Daten – insbesondere der Anschrift der Schülerinnen und Schüler – auch nicht erforderlich, um den Zweck des Monitorings zu erreichen.

Datenschutzkonforme Alternative

Nach Rücksprache mit dem Schulträger stellte sich heraus, dass das Ziel des Monitorings auch dann erreicht werden kann, wenn nicht die Adresse der Schülerinnen und Schüler, sondern ein übergeordnetes Merkmal erhoben wird, wie z. B. das Stadtviertel oder der Ortsteil, in dem die Betroffenen leben.

Auf diese Weise kann anhand eines einzelnen Datensatzes kein Personenbezug mehr hergestellt werden, sodass sowohl dem Ziel des Monitorings als auch dem Schutz der personenbezogenen Daten der Schülerinnen und Schüler gleichermaßen Rechnung getragen wird. Der Schulträger plante bei Redaktionsschluss, zu diesem alternativen Monitoring-Modell zu wechseln. Inwieweit der Plan bereits umgesetzt worden ist, kann ich derzeit nicht beurteilen.

5.2 Antworten zum Einsatz von Videokonferenzsystemen in Schulen

Aufgrund der Corona-Pandemie wurde von den niedersächsischen Schulen zwischenzeitlich verstärkt Distanzunterricht angeboten. Als Kommunikationsplattform nutzten Schulen häufig Videokonferenzsys-teme (VKS). Bei Videokonferenzen wird eine Vielzahl personenbezoge-ner Daten verarbeitet, sodass datenschutzrechtliche Belange berücksichtigt werden müssen. Um die Schulen in dieser herausfordernden Situation zu unterstützen, habe ich gemeinsam mit den Regionalen Landesämtern für Schule und Bildung eine Übersicht häufig gestellter Fragen und Antworten zum Einsatz von VKS in Schulen (FAQ) erstellt.

Grundsätzlich darf eine Schule unter anderem dann personenbezogene Daten von Schülerinnen und Schülern sowie Lehrkräften mit Hilfe digitaler Lehr- und Lernmittel (z. B. VKS) verarbeiten, wenn dies zur Erfüllung des Bildungsauftrags der Schule erforderlich ist. Dazu gehört zum Beispiel die Durchführung des Unterrichts. Diese Erforderlichkeit war während des pandemiebedingten Ausfalls des Präsenzunterrichts gegeben.

FAQ VKS:
https://t1p.de/FAQ-VKS

Verarbeitet werden dürfen insbesondere:

- die IP-Adresse der Teilnehmerinnen und Teilnehmer,
- die Bild- und Tonübertragung der Teilnehmerinnen und Teilnehmer,
- geteilte Dateien,
- der Nachrichtenaustausch unter den Teilnehmerinnen und Teilnehmern während der Videokonferenz (Chats)

Neben Informationen zur rechtlichen Grundlage des VKS-Einsatzes an Schulen beantworten die FAQ Fragen die sich speziell für Schülerinnen und Schüler, Erziehungsberechtigte sowie für die Lehrkräfte ergeben.

Technische Eckpunkte:
https://t1p.de/Technische-Eckpunkte-VKS

Die „Technischen Eckpunkte für den Einsatz von Videokonferenzsystemen an Schulen“ ergänzen dieses FAQ um zentrale Aspekte des technisch-organisatorischen Datenschutzes. Auf diese Weise bieten die FAQ den Schulen eine Hilfestellung, damit Videokonferenzsysteme datenschutzkonform im Unterricht genutzt werden können.

5.3 Weiterhin keine Freigabe für die Niedersächsische Bildungscloud

Im September 2021 hat mir das Niedersächsische Kultusministerium erneut eine überarbeitete Fassung des Datenschutzkonzepts zur Niedersächsischen Bildungscloud (NBC) übersandt, die auch eine Datenschutz-Folgenabschätzung enthielt. Aufgrund fortbestehender, bereits in der Vergangenheit angemerkter Änderungs- und Ergänzungsbedarfe des Datenschutzkonzepts, konnte eine Freigabe der NBC aus datenschutzrechtlicher Sicht nicht erfolgen.

Die Unterlagen wurden von mir dahingehend geprüft, ob die bereits im Dezember 2020 mitgeteilten datenschutzrechtlichen Änderungs- und Ergänzungsbedarfe berücksichtigt worden waren. Meine Prüfung ergab, dass die dem Kultusministerium teils hinlänglich bekannten Mängel sowohl im rechtlichen Bereich als auch im Bereich der Datenschutz-Folgenabschätzung größtenteils nicht beseitigt worden waren, sodass eine datenschutzrechtliche Freigabe der NBC anhand der mir vorliegenden Unterlagen nicht möglich war.

Die wesentlichen Beanstandungen waren:

- Die Struktur und das Zusammenspiel der an der NBC beteiligten Akteure war nach wie vor unklar. Insbesondere waren Teile des Datenschutzkonzepts nicht an den Umstand angepasst worden, dass das Hasso-Plattner-Institut als ursprünglicher Hauptakteur der NBC im Verlauf des Berichtsjahres durch den IT-Dienstleister Dataport ersetzt worden war.

Grundlage für Übermittlung an Dritte fehlt

- Aus den Unterlagen ergab sich, dass personenbezogene Daten an außerhalb der NBC stehende Dritte übermittelt werden sollten. Es wurde jedoch weder eine gesetzliche Rechtsgrundlage benannt, auf die die Übermittlung gestützt werden könnte, noch war eine solche erkennbar.
- Es blieb nach wie vor offen, wie und durch wen an die NBC angeschlossene Produkte (Lern- und Bildungsinhalte) externer Anbieter vorab auf Datenschutzkonformität geprüft werden.
- Die eingereichte Datenschutz-Folgenabschätzung war unvollständig und wies in Bezug auf entscheidende Punkte Mängel auf.

Offizieller Abschluss der Prüfung

Ich übermittelte dem Kultusministerium das Ergebnis meiner Prüfung und bat darum, die mitgeteilten Änderungsbedarfe zeitnah in eigener Zuständigkeit umzusetzen. Gleichzeitig wies ich darauf hin, dass die Umsetzung dieser Änderungen auch für die Erfüllung der Informationspflichten gemäß Art. 13 und 14 Datenschutz-Grundverordnung (DS-GVO) gegenüber den betroffenen Schülerinnen und Schülern sowie Lehrkräften durch die jeweils datenschutzrechtlich verantwortliche Schule unabdingbar ist. Hinzukommt, dass die Schule im Zuge der ihr obliegenden Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO den datenschutzkonformen Einsatz der NBC nachweisen muss. Dies setzt jedoch ein vollständiges und nachvollziehbar strukturiertes Datenschutzkonzept voraus.

Schulen müssen Rechenschaftspflicht einhalten

Schließlich teilte ich dem Kultusministerium mit, dass ich vor dem Hintergrund der umfangreichen, über einen langen Zeitraum und mit hohem Aufwand geleisteten Beratungen keine erneute Prüfung ggf. überarbeiteter Unterlagen durchführen kann.

Eckpunkte für Bildungsplattformen geplant

Die gewonnenen Erkenntnisse aus der datenschutzrechtlichen Begleitung der NBC werde ich in die noch in der Entwicklung befindlichen „Eckpunkte für den datenschutzkonformen Einsatz von Bildungsplattformen im Schulbereich“ einfließen lassen, die den Schulen als Hilfestellung beim Einsatz von Bildungsplattformen dienen sollen.

5.4 Datenschutzkonforme Online-Prüfungen an Hochschulen

Digitale Prüfungsformate können im Einklang mit dem geltenden Datenschutzrecht eingesetzt werden. Dabei unterstützen sollen die von meiner Behörde entwickelten Eckpunkte für Online-Prüfungen in den Hochschulen.

Die niedersächsischen Hochschulen mussten pandemiebedingt nicht nur ihre Lehrveranstaltungen, sondern auch ihre Prüfungen in digital durchführen. Da Online-Prüfungen im Vergleich zu herkömmlichen analogen Prüfungen höhere Risiken für die Privatsphäre der Prüflinge bergen, verschaffte ich mir im Sommersemester 2021 durch eine Umfrage an den niedersächsischen Hochschulen einen Überblick über die eingesetzten Verfahren. Dabei stellte ich fest, dass die Hochschulen weitgehend datenschutzkonform agierten.

Da davon auszugehen ist, dass Online-Prüfungen auch nach Ende der Pandemie zumindest in einigen Studiengängen dauerhaft erhalten bleiben, entwickelte ich praxisorientierte Eckpunkte für den datenschutzkonformen Einsatz solcher Prüfungen in den niedersächsischen Hochschulen. Inhaltlich geht es darin insbesondere um Maßnahmen zur Identitätsfeststellung der Studierenden, um den Einsatz von Kameras zur Prüfungsüberwachung sowie um die Unzulässigkeit konkreter Überwachungsmaßnahmen oder -programme. Zudem werden weitere Anforderungen beschrieben, die aus der unmittelbaren Geltung der Datenschutz-Grundverordnung folgen. Dies betrifft insbesondere den Einsatz externer Dienstleister und die Regelungen des internationalen Datentransfers.

Eckpunkte für Online-Prüfungen:
https://t1p.de/Eckpunkte-Onlinepruefungen

Mit diesen Eckpunkten wird Rechtssicherheit für die Hochschulen geschaffen. Zugleich wird der Schutz der Privatsphäre der Studierenden bei digitalen Prüfungsformaten sichergestellt.

J.6. Wirtschaft

6.1 Nachkontrollen zur Querschnittsprüfung in der niedersächsischen Wirtschaft

Im Jahr 2021 konnte ich fast alle Nachkontrollen meiner Querschnittsprüfung von Wirtschaftsunternehmen abschließen, die ich 2018 begonnen hatte. Dies betraf Unternehmen, die erhebliche Defizite bei der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) gezeigt hatten. Bei den Vor-Ort-Kontrollen hatten einige Unternehmen bereits die identifizierten Defizite behoben, andere hatten sich hingegen nur unzureichend oder gar nicht auf die Prüfung vorbereitet, was entsprechend umfangreiche aufsichtsrechtliche Verfahren zur Folge hatte.

Meine Erfahrungen mit Vor-Ort-Kontrollen bewerte ich als sehr positiv, da sie mir einen tiefergehenden und umfassenderen Einblick in die Umsetzung der DS-GVO erlauben als eine ausschließlich schriftliche Prüfung. Ich möchte an dieser Stelle überblickartig darstellen, welche Arten von Verstößen ich bei diesen Kontrollen festgestellt habe und wie sorgfältig eine Vor-Ort-Kontrolle vorbereitet werden sollte, damit sich niedersächsische Unternehmen in Zukunft besser auf diese Art der Überprüfung einstellen können.

Festgestellte Verstöße

Fitnessstudio speichert Zutrittszeit ohne Rechtsgrundlage

Eine Verarbeitungstätigkeit eines Fitnessstudios untersagte ich und wies die Löschung von personenbezogenen Daten an, weil mir keine Rechtsgrundlage nachgewiesen wurde und auch ich keine erkennen konnte. So erfasste das eingesetzte Zugangssystem den Zeitpunkt des Betretens durch die Kundinnen und Kunden und speicherte dies in einer Datenbank ab. Ich gab dem Betreiber Gelegenheit, mir das Vorliegen einer Rechtsgrundlage für diese Verarbeitung nachzuweisen. Daraufhin wurde unter anderem pauschal vorgetragen, die Verarbeitung diene der Zugangskontrolle, sei zur Wahrung des Hausrechts, zur Wahrung der Interessen der Mitglieder und zur Verteidigung gegen Rechtsansprüche erforderlich.

Für eine Zugangskontrolle ist es in diesem Fall jedoch lediglich erforderlich, beim Betreten zu prüfen, ob eine Person Kundin oder Kunde ist. Eine Speicherung des Zeitpunktes des Betretens ist nicht erforderlich. Zu seinen weiteren Begründungen erläuterte der Verantwortliche nicht, inwiefern die Zeiterfassung zur Erreichung dieser unkonkreten Zwecke erforderlich ist oder warum eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zu seinen Gunsten ausgeht. In diesem Fall, in dem auch weitere Verstöße festgestellt worden waren, ordnete ich deren Abhilfe an, leitete zudem ein Ordnungswidrigkeitenverfahren ein und prüfe die Verhängung einer Geldbuße.

Mängel in Verträgen zur Auftragsverarbeitung

Auffällig war auch das Thema Auftragsverarbeitung. Die geprüften Verantwortlichen hatten teilweise keine Übersicht darüber, welche Unternehmen für sie Verarbeitungen im Auftrag durchführen, konnten nicht für jedes dieser Unternehmen einen Auftragsverarbeitungsvertrag vorlegen oder die Verträge waren veraltet und entsprachen nicht mehr dem tatsächlichen Umfang der Verarbeitung. Auch hierzu ergingen von mir Anordnungen, wenn im laufenden Verfahren eine Nachbesserung unterblieb.

Immer wieder gab es in den Medien während des Berichtszeitraums Meldungen über Cyberangriffe auf Unternehmen, die erhebliche Schäden verursachen und zu Reputationsverlusten führen. Obwohl es daher eigentlich auch im eigenen Interesse der Unternehmen wäre, ihre Informationstechnik auf einem hohen Sicherheitsniveau zu betreiben, war dies nicht überall der Fall. Unternehmen, die personenbezogene Daten verarbeiten, müssen angemessene Maßnahmen treffen, damit Vertraulichkeit, Integrität und Verfügbarkeit dieser Daten geschützt und die Grundsätze des Datenschutzes aus Art. 5 Abs. 1 DS-GVO umgesetzt werden. Wie angemessene technisch-organisatorische Maßnahmen bestimmt und implementiert werden, habe ich mit dem Prozess ZAWAS dargestellt.

Prozess ZAWAS: https://t1p.de/ZAWAS

Auch wenn die datenschutzrechtlichen Normen ausschließlich dem Schutz der betroffenen Personen dienen, können Unternehmen zwei Fliegen mit einer Klappe schlagen, indem sie die datenschutzrechtlichen Vorgaben erfüllen und gleichzeitig weniger anfällig für Cyberangriffe werden.

Unter den identifizierten Mängeln sind folgende hervorzuheben:

- fehlende oder veraltete Übersicht darüber, welche Hard- und Software verwendet wird
- Abweichungen zwischen der Dokumentation und den tatsächlich implementierten technisch-organisatorischen Maßnahmen
- unsichere oder fehlende Verschlüsselung von personenbezogenen Daten, obwohl dies umsetzbar und angesichts der Risiken erforderlich ist
- fehlende oder ungenügende Berechtigungskonzepte
- fehlende Löschkonzepte
- fehlende Passwortrichtlinien
- fehlende Datensicherungskonzepte

Sorgfältig auf die Prüfung vorbereiten

Bei den Vor-Ort-Kontrollen und im nachfolgenden weiteren Verfahren war ein deutlicher Unterschied zwischen Unternehmen zu verzeichnen, die zwar noch im Rahmen der Querschnittsprüfung schlecht abgeschnitten hatten, dann jedoch die Zeit zur Vorbereitung auf die Vor-Ort-Kont-

rolle genutzt hatten und denjenigen Unternehmen, die sich nicht oder nur unzureichend mit den datenschutzrechtlichen Anforderungen beschäftigt hatten.

Wird eine Vor-Ort-Kontrolle angekündigt, sollten sich Unternehmen im eigenen Interesse sorgfältig darauf vorbereiten.

Das können Unternehmen vor der Vor-Ort-Kontrolle tun

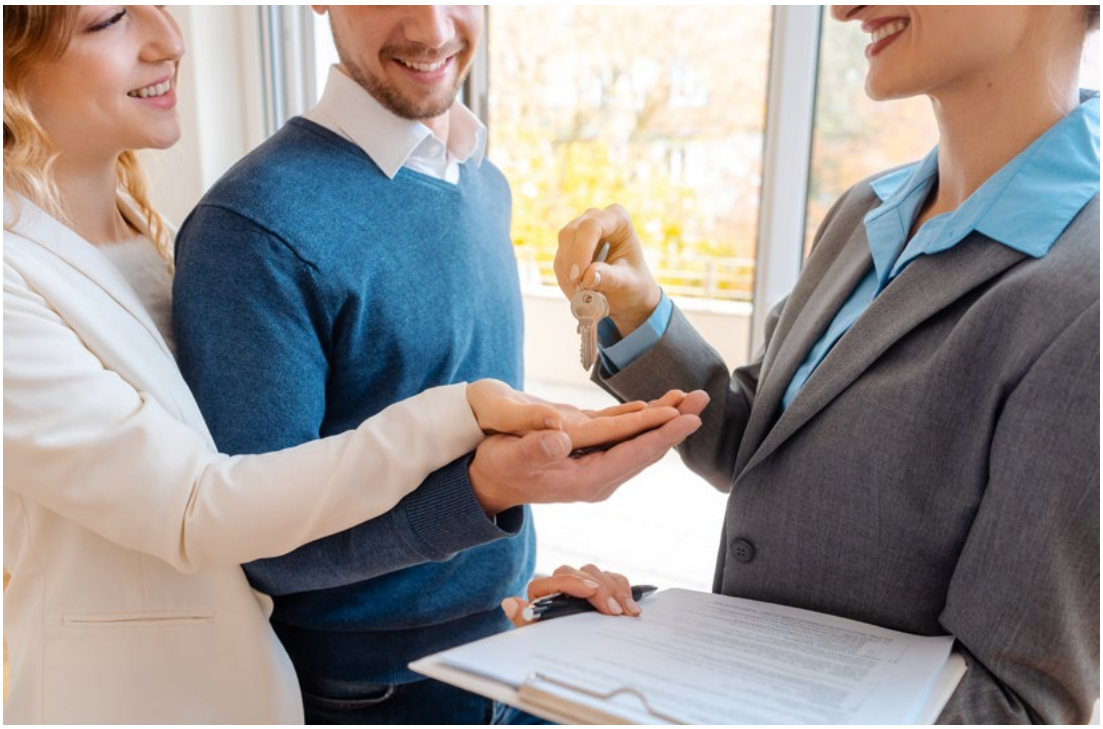
Es ist insbesondere ratsam,

- die vorhandene Datenschutzdokumentation zu sichten, Lücken zu identifizieren und zu füllen;
- zu prüfen, ob die Dokumente aktuell sind oder ob sich seit der Erstellung der Dokumente Veränderungen ergeben haben, die noch nicht berücksichtigt wurden;
- die Dokumentation so zu ordnen, dass während der Vor-Ort-Kontrolle Unterlagen auf Anfrage unmittelbar vorgelegt werden können;
- die eigene Dokumentation auf Widersprüche zu prüfen;
- Abweichungen von den einschlägigen Veröffentlichungen meiner Behörde, der Datenschutzkonferenz und des Europäischen Datenschutzausschusses zu prüfen;
- den Datenschutzbeauftragten des Unternehmens bei der Vorbereitung eng einzubinden;
- ggf. einen externen Datenschutzberater einen unbefangenen Blick auf die Umsetzung des Datenschutzrechts im Unternehmen werfen zu lassen;
- die Verfügbarkeit der Verantwortlichen aus den jeweiligen Fachbereichen für den Kontrolltermin sicherzustellen, die tiefergehende Nachfragen zu einzelnen Verarbeitungstätigkeiten beantworten können;
- einen Umsetzungsplan zu erstellen, welcher der Aufsichtsbehörde vorgelegt werden kann, falls bis zur Vor-Ort-Kontrolle nicht alle Dokumente erstellt oder technisch-organisatorischen Maßnahmen implementiert werden konnten.

Wie anschließend das weitere Verfahren verläuft und ob es zu einem Bußgeld und/oder aufsichtsbehördlichen Maßnahmen kommt, ist immer eine Frage des Einzelfalls und hängt von den in der Vor-Ort-Kontrolle gemachten Feststellungen ab.

Stelle ich bei einer Vor-Ort-Kontrolle fest, dass das Unternehmen ein umfassendes Datenschutz-Management implementiert hat, ist es im Nachgang oft nicht erforderlich von den aufsichtsbehördlichen Befugnissen aus Art. 58 Abs. 2 DS-GVO Gebrauch zu machen oder es ist ausreichend, eine Verwarnung auszusprechen. Vereinzelte, nicht besonders schwerwiegende Mängel können dann nach der Kontrolle behoben und mir nachgewiesen werden. Ist hingegen nicht absehbar, wann und wie Mängel abgestellt werden sollen oder werden gravierende Mängel festgestellt, lassen sich aufsichtsbehördliche Maßnahmen nur noch schwer vermeiden.

6.2 Abfrage von personenbezogenen Daten durch Vermieter



Bevor ein Vermieter sich entscheidet, welchem der zahlreichen Interessenten er eine Wohnung vermietet, verschafft er sich eine Entscheidungsgrundlage und erhebt dafür häufig eine Vielzahl von personenbezogenen Daten. Allerdings dürfen nur die Daten erhoben werden, die für diese Entscheidung erforderlich sind. Im Berichtszeitraum haben mich zahlreiche Eingaben von Bürgerinnen und Bürgern erreicht, die zeigen, dass teilweise von Vermietern deutlich mehr Daten erhoben werden als notwendig und zulässig ist.

Eine Bürgerin wandte sich an mich, weil Sie einen Besichtigungstermin vereinbaren wollte und die potenzielle Vermieterin ihr einen umfangreichen Fragenkatalog zugesandt hatte. Darin wurde neben den Kontaktdaten auch Daten zum Beschäftigungsverhältnis inklusive Kopien von Gehaltsnachweisen, zur Staatsangehörigkeit, die Kontaktdaten des Arbeitgebers und eine Personalausweiskopie angefordert. Die Vermieterin konnte nach Einleitung eines aufsichtsrechtlichen Verfahrens glaubhaft darlegen, dass sie in diesem Fall nur

ausnahmsweise aufgrund der hohen Anzahl von Interessentinnen und Interessenten für das fragliche Mietobjekt so vorgegangen war und in Zukunft nicht mehr so verfahren würde. Daher waren hier weitergehende aufsichtsbehördliche Maßnahmen nicht erforderlich.

In einem anderen Fall wurde bereits vor der Vereinbarung eines Besichtigungstermins durch den Vermieter die Vorlage einer Personalausweiskopie, einer Schufa-Auskunft, einer Kopie des Arbeitsvertrages und sogar eines polizeilichen Führungszeugnisses verlangt. Dies ist im Regelfall unzulässig. Das aufsichtsbehördliche Verfahren konnte im Berichtszeitraum nicht abgeschlossen werden.

Rechtliche Vorgaben

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat bereits 2018 eine Orientierungshilfe veröffentlicht, in der die datenschutzrechtlichen Rahmenbedingungen bei der Anbahnung eines Mietverhältnisses erläutert werden.

Orientierungshilfe der DSK: https://t1p.de/Mietauskuenfte

Einige Punkte möchte ich an dieser Stelle noch einmal hervorheben:

- Vor einem Besichtigungstermin ist es grundsätzlich nicht erforderlich, Daten zu den wirtschaftlichen Verhältnissen zu erheben. Es können lediglich Kontaktdaten und ggf. Angaben zu einem Wohnberechtigungsschein erhoben werden.
- Möchte ein Interessent die Wohnung nach dem Besichtigungstermin anmieten, können weitergehende Informationen, insbesondere zur Beurteilung der Bonität des Interessenten, erhoben werden. Allerdings dürfen unter anderem folgende Informationen und Unterlagen weiterhin grundsätzlich nicht erhoben werden:
  - Religion, ethnische Herkunft und Staatsangehörigkeit
  - Vorstrafen und strafrechtliche Ermittlungsverfahren
  - Heiratsabsichten, Schwangerschaften und Kinderwünsche
  - Mitgliedschaften in Parteien und Mietvereinen
  - Dauer des Beschäftigungsverhältnisses
  - Kontaktdaten früherer Vermieter
  - Personalausweiskopien

6.3 Beschäftigtendaten im Kündigungsschutzprozess

Ein Mitarbeiter, dem fristlos gekündigt worden war, setzte sich vor dem zuständigen Arbeitsgericht zur Wehr. Hierzu beantragte er den Erlass einer einstweiligen Verfügung gegen die Arbeitgeberin mit dem Ziel, weiterbeschäftigt zu werden. Dabei offenbarte er dem Arbeitsgericht ohne Grund und ohne Rechtsgrundlage Einzelheiten aus den Beschäftigungsverhältnissen mehrerer Kolleginnen und Kollegen.

Zur Kenntnis gelangte mir diese Datenverarbeitung des Mitarbeiters durch eine Meldung der Arbeitgeberin nach Art. 33 Abs. 1 DS-GVO, nachdem sie von der Offenbarung erfahren hatte.

Auf meine Nachfrage teilte die Arbeitgeberin mit, sie habe die Erhebung der personenbezogenen Daten der Beschäftigten durch den Mitarbeiter nicht abschließend klären können. Sie konnte jedoch glaubhaft machen, dass die Tätigkeit des Mitarbeiters weder die Kenntnisnahme noch die darüberhinausgehende Nutzung von Einzelheiten aus den Beschäftigungsverhältnissen der Kolleginnen und Kollegen erforderte. Vor diesem Hintergrund war die Offenbarung der personenbezogenen Daten gegenüber dem Arbeitsgericht nicht der Arbeitgeberin, sondern dem ehemaligen Mitarbeiter als datenschutzrechtlich Verantwortlichen zuzurechnen, da er damit den ihm zugewiesenen Verantwortungsbereich deutlich verlassen hatte und so selbst zum Verantwortlichen im Sinne der DS-GVO geworden war (sog. Mitarbeiterexzess). Mit Blick auf die Art und Anzahl der betroffenen personenbezogenen Daten der Beschäftigten wurde gegen ihn ein Prüfverfahren eingeleitet.

Prüfverfahren wegen Exzesses des Mitarbeiters

DS-GVO auch bei Rechtsverfolgung

Die DS-GVO ist auch auf die Verarbeitung personenbezogener Daten anwendbar, die im Zusammenhang mit einem Kündigungsschutzprozess und damit zur Rechtsverfolgung erfolgt. Die sogenannte Haushaltsausnahme steht dem nicht entgegen.

Keine Haushaltsausnahme

Als Haushaltsausnahme wird die Regelung des Art. 2 Abs. 2 Buchstabe c DS-GVO bezeichnet. Nach dieser Vorschrift finden datenschutzrechtliche Vorschriften auf solche Datenverarbeitungen keine Anwendung, die Personen ausschließlich im Kontext rein privater oder familiärer Tätigkeiten vornehmen. Hiervon ist entsprechend des Erwägungsgrundes Nr. 18 auszugehen, wenn der Datenverarbeitung jedweder Bezug zu einer beruflichen oder wirtschaftli-

chen Tätigkeit fehlt. Bei der Annahme einer solchen Tätigkeit ist Zurückhaltung geboten, um das Schutzniveau, der DS-GVO, nicht zu unterlaufen.

Datenverarbeitungen, die im Kontext eines Kündigungsschutzprozesses erfolgen, haben einen beruflichen Bezug. Es entspricht auch dem Willen des Verordnungsgebers, die DS-GVO auf Datenverarbeitungen anzuwenden, die der Rechtsverfolgung dienen. Der Verordnungsgeber hat die Rechtsverfolgung und -verteidigung als Zweck einer Datenverarbeitung in mehreren Regelungen der DS-GVO erwähnt.

Datenverarbeitung auf das Notwendige begrenzen

Das gegen den Mitarbeiter eingeleitete Prüfverfahren ergab, dass die Offenbarung der Einzelheiten aus den Beschäftigungsverhältnissen der Kolleginnen und Kollegen gegenüber dem Arbeitsgericht ohne Rechtsgrundlage und damit unrechtmäßig erfolgte. Andere Rechtsgrundlagen als die des Art. 6 Abs. 1 Buchstabe f DS-GVO (Interessenabwägung) kamen nicht in Betracht. Die Prüfung ergab, dass die Voraussetzungen dieser Rechtsgrundlage nicht erfüllt waren. Zwar stand die Offenbarung im Kontext der Rechtsverfolgung und -verteidigung und konnte zur Wahrung eines berechtigten Interesses ausgelegt werden. Es fehlte jedoch im vorliegenden Fall bereits im Ansatz die Erforderlichkeit der Offenlegung zur Rechtsverfolgung und -verteidigung.

Erforderlichkeit ist eng auszulegen

Zur Bestimmung des Begriffs der Erforderlichkeit orientierte ich mich am Beschluss des OVG Lüneburg vom 19. Januar 2021 (Az. 11 LA 16/20): Unter Berücksichtigung von Erwägungsgrund 39 Satz 9 DS-GVO besteht eine Erforderlichkeit, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Im Gegensatz zum weit auszulegenden Begriff der „berechtigten Interessen“ ist der Begriff der Erforderlichkeit eng auszulegen. Zur Bejahung der Erforderlichkeit reicht somit weder eine bloße Zweckdienlichkeit oder eine bestmögliche Effizienz der Datenverarbeitung, noch kann die Erforderlichkeit allein damit begründet werden, dass es sich bei der beabsichtigten Datenverarbeitung um die aus Sicht des Verantwortlichen wirtschaftlich sinnvollste Alternative handelt. Kann das Ziel einer Datenverarbeitung auch durch die Verarbeitung anonymisierter Daten erreicht werden, ist eine offene Verarbeitung nicht erforderlich. Die Datenverarbeitung ist auf das „absolut Notwendige“ zu begrenzen.

Aus dem Antrag des Mitarbeiters auf Erlass einer einstweiligen Verfügung ging nicht hervor, welche Relevanz die Einzelheiten aus den Beschäftigungsverhältnissen der Kolleginnen und Kollegen für die Wirksamkeit der Kündigung des Arbeitsverhältnisses zwischen ihm und der Arbeitgeberin hatten. Dies konnte der Mitarbeiter auch im Prüfverfahren nicht darlegen. Auch meine Behörde vermochte im vorliegenden Fall den Bezug der Mitteilung der personenbezogenen Daten zum Rechtsstreit nicht zu erkennen, diese waren für das gerichtliche Verfahren ohne jeglichen Belang. Es lag bereits keine Zweckdienlichkeit vor. Vor diesem Hintergrund sowie der weiteren Umstände des Einzelfalls war hier eine datenschutzrechtliche Sensibilisierung durch Ausspruch einer Verwarnung notwendig und geboten.

6.4 E-Mail-Werbung durch Online-Händler – Zusammenspiel von Wettbewerbs- und Datenschutzrecht

Auch im Jahr 2021 haben mich zahlreiche Beschwerden zur E-Mail-Werbung erreicht. Häufig machen es Verantwortliche den betroffenen Personen dabei schwer, ihre Widerspruchsrechte wahrzunehmen.

Im Kontext einer grenzüberschreitenden Beschwerde, die ich als federführende Behörde gem. Art. 56 Abs. 3 Satz 2 Datenschutz-Grundverordnung (DS-GVO) prüfte, stellte ich fest, dass Personen bei Bestellungen in Online-Shops oftmals verpflichtet werden, eine E-Mail-Adresse für Werbezwecke anzugeben.

Grundsätzlich ist E-Mail-Werbung an Neukunden und-kundinnen nur dann datenschutzkonform, wenn vorab eine Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DS-GVO eingeholt wurde. Soweit es sich um E-Mail-Werbung an Bestandskundeninnen und -kunden handelt, kann die Verarbeitung der E-Mail-Adresse auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden. Die Verwendung von E-Mail-Adressen, die im Verlauf einer Geschäftsbeziehung für Werbezwecke erhoben wurden, ist grundsätzlich nach Art. 6 Abs. 1 lit. f DS-GVO zulässig, wenn zugleich die Vorgaben des Art. 7 Abs. 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) für elektronische Werbung eingehalten werden.

Orientierungshilfe der DSK zur Direktwerbung: https://t1p.de/OH-Werbung

Ausführungen im Wettbewerbsrecht

Bei dem im Berichtszeitraum näher untersuchten Vorgang war zunächst fraglich, ob die Voraussetzungen des § 7 Abs. 3 UWG durch das Unternehmen eingehalten wurden. Zum Widerspruchsrechts ist dort geregelt, dass Kundinnen und Kunden der Verwendung nicht widersprochen haben dürfen und bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen werden, dass sie der Verwendung jederzeit widersprechen können.

Berücksichtigung des § 7 Abs. 3 UWG bei Auslegung des Art. 6 Abs. 1 lit. f DS-GVO

Das Unternehmen trug mir gegenüber vor, dass es die Vorgaben des § 7 Abs. 3 UWG erfülle, indem es beim Zeitpunkt der Erhebung und auch in jeder Werbe-E-Mail über das Widerspruchsrecht informiere.

§ 7 Abs. 3 UWG setzt Art. 13 der Richtlinie 2002/58/EG um. Art. 13 Abs. 2 der Richtlinie sieht jedoch vor, dass die Kundinnen und Kunden zum Zeitpunkt der

Erhebung die Möglichkeit erhalten, die Nutzung der elektronischen Kontaktinformationen problemlos abzulehnen. Bei europarechtskonformer Auslegung von § 7 Abs. 3 UWG ist es also nicht ausreichend, Kundinnen und Kunden lediglich auf das Widerspruchsrecht hinzuweisen, sondern es muss ihnen unmittelbar eine problemlose Widerspruchsmöglichkeit bei der Erhebung eingeräumt werden.

Erleichterungsgebot des Art. 12 Abs. 2 S. 1 DS-GVO

Im konkreten Fall kam es nicht darauf an, ob eine solche europarechtskonforme Auslegung geboten ist. Es stellte sich im Verlauf des Verfahrens heraus, dass bereits die damalige Ausgestaltung der Erhebung von E-Mail-Adressen im Online-Shop des Unternehmens gegen Art. 12 Abs. 2 S. 1 i.V.m. 21 Abs. 2 DS-GVO verstieß. Danach hat der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte gemäß den Artikeln 15 bis 22 DS-GVO zu erleichtern. Dieses Erleichterungsgebot umfasst die Ausübung des Werbewiderspruchs nach Art. 21 Abs. 2 DS-GVO. Die Pflicht zur Erleichterung geht über ein bloßes Behinderungsverbot hinaus und umfasst auch die Bereitstellung von einfachen Interaktionsmöglichkeiten.[1]

Umsetzung des Erleichterungsgebots durch Auswahlkästchen

Art. 12 Abs. 2 S. 1 DS-GVO ist bei der von dem Unternehmen vorgenommenen Erhebung von E-Mail-Adressen während des Bestellvorgangs dadurch umzusetzen, dass ein Auswahlkästchen eingebunden wird, mit dem die betroffene Person unmittelbar im Zusammenhang mit der Erhebung der E-Mail-Adresse der Verwendung zu Werbezwecken widersprechen kann. Eine solche Auswahlmöglichkeit bot das Unternehmen jedoch nicht an.

Angabe einer E-Mail-Adresse für Widerspruch reicht nicht aus

Die Angabe einer E-Mail-Adresse, an die ein Widerspruch gerichtet werden kann, wäre in diesem Fall auch nicht ausreichend, da die betroffene Person sich zunächst in ihren E-Mail-Account einloggen oder ihr E-Mail-Programm öffnen müsste, anschließend eine E-Mail mit dem Widerspruch formulieren und diese absenden müsste. Dies würde gegenüber dem Ankreuzen eines Ankreuzkästchens einen erheblichen Mehraufwand darstellen, der die betroffene Person von einem Widerspruch abhalten könnte und würde daher nicht die Pflicht zur Erleichterung der Ausübung der Betroffenenrechte nach Art. 12 Abs. 2 DS-GVO erfüllen. Nicht ausreichend wäre es zudem, das Ankreuzkästchen erst dann anzuzeigen, wenn eine Linkfläche „Verwendung deiner E-Mail-Adresse für Werbezwecke“ aktiv angeklickt wurde, da dies die Ausübung der Rechte ebenfalls erschweren würde.

Meine Behörde wies das Unternehmen in diesem Zusammenhang darauf hin, ein entsprechendes Auswahlkästchen einzubinden. Das Unternehmen aktualisierte kurze Zeit später seine Webseite. Es gestaltete die Erhebung der E-Mail-Adresse nun rechtskonform aus, indem es das geforderte Auswahlkästchen in seinen Online-Shops integrierte, mit welchem Kundinnen und Kunden der Verwendung ihrer E-Mail-Adresse für Werbezwecke widersprechen können.

1 vgl. Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 12 Rn. 23;

6.5 GPS-Ortung von Beschäftigten

Regelmäßig erreichen mich Beschwerden von Bürgerinnen und Bürgern, die von ihren Arbeitgeberinnen und Arbeitgebern per GPS geortet werden. In fast allen Fällen ist die GPS-Ortung rechtswidrig, weil sie für die verfolgten Ziele nicht erforderlich ist.

Im Rahmen eines bestehenden Arbeitsvertrages dürfen Arbeitgeberinnen und Arbeitgeber Beschäftigtendaten nach § 26 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes (BDSG) 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 erforderlich sein.

Unter den Begriff „verarbeiten" fallen laut der Definition in Artikel 4 Nummer 2 der Datenschutz-Grundverordnung (DS-GVO) unter anderem die Erhebung und Nutzung von Beschäftigtendaten. Hierzu zählt auch die Erhebung und Nutzung mittels GPS erhobener Positionsdaten von Beschäftigten.

Die unternehmerische Freiheit erlaubt es 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.

Gesetzliche Voraussetzungen liegen nicht vor

Arbeitgeberinnen und Arbeitgeber geben häufig an, mittels der GPS-Ortung ihrer Beschäftigten Arbeitsabläufe bestimmen zu wollen oder aber berechtigte Interessen zu verfolgen, unter anderem: Tourenplanung, Mitarbeiter- und Mitarbeiterinneneinsatz, präventiver Diebstahlschutz für die eingesetzten Firmenfahrzeuge oder zum Nachweis für geleistete Tätigkeiten gegenüber Vertragspartnern.

Urteil VG Lüneburg (Kurzlink): https://t1p.de/UrteilVG

Jedoch ist die GPS-Ortung von Beschäftigten in der Regel hierfür nicht erforderlich. Dies hat das Verwaltungsgericht Lüneburg bereits mit Urteil vom 19. März 2019 (Aktenzeichen 4 A 12/19) festgestellt. Hierüber habe ich bereits in meinem 25. Tätigkeitsbericht berichtet. Zwischenzeitlich ist das Urteil mit Beschluss des Oberverwaltungsgerichts Lüneburg vom 3. April 2020 (Aktenzeichen 11 LA 154/19) rechtskräftig geworden.

In der Regel ist eine GPS-Ortung von Beschäftigten auch nicht aufgrund von berechtigten Interessen von Arbeitgeberinnen und Arbeitgebern möglich. Auch wenn Diebstahlsschutz sowie eine Beweisführung gegenüber Vertragspartnern berechtigte Interessen darstellen, ist eine fortlaufende GPS-Ortung der Beschäftigten nicht geeignet, Diebstähle zu verhindern. Die in der Vergangenheit erhobenen Positionsdaten der Beschäftigten können nicht dazu führen, die aktuelle Position des Täters zu bestimmen. Daher würde es ausreichen, die GPS-Ortung erst nach einem Diebstahl zu aktivieren. Weiter wird durch die GPS-Ortung der Beschäftigten gegenüber Vertragspartnern nicht nachgewiesen, dass eine Leistung tatsächlich erbracht worden ist, sondern allenfalls, dass ein Beschäftigter sich möglicherweise am Leistungsort befand.

Positionsdaten sagen nichts über Leistungserfüllung aus

Ortung mit Einwilligung der Beschäftigten?

Immer wieder behaupten Arbeitgeberinnen und Arbeitgeber, dass die GPS-Ortung ihrer Beschäftigten mit deren Einwilligung erfolgt. Um rechtswirksam zu sein, muss diese Einwilligung aber freiwillig erteilt worden sein. Tatsächlich freiwillig wird eine Einwilligung aber selten sein, weil zwischen Arbeitgeberinnen und Arbeitgebern ein Über- und Unterordnungsverhältnis herrscht. Beschäftigte willigen häufig nicht freiwillig ein, sondern weil sie andernfalls Nachteile befürchten.

Das Gesetz nennt Indizien, wann von einer Freiwilligkeit der Einwilligung eines Beschäftigten ausgegangen werden kann: Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen (§ 26 Absatz 2 Satz 2 BDSG). Diese Indizien sind häufig nicht gegeben.

Freiwillige Einwilligung ist im Beschäftigungsverhältnis schwierig

Die Freiwilligkeit und damit Rechtswirksamkeit einer Einwilligung von Beschäftigten in die Verarbeitung ihrer Positionsdaten nehme ich zum Beispiel nur dann an, wenn den Beschäftigten hierfür ein Vorteil, wie die private Nutzung der Firmenfahrzeuge, gewährt worden ist und weitere Indizien für die Freiwilligkeit der Einwilligung in die Datenverarbeitung vorlagen. Zum Beispiel, wenn die Beschäftigten die Möglichkeit hatten, das am Firmenfahrzeug angebrachte GPS-Ortungsgerät selbständig auszuschalten. Dabei ist zu beachten, dass Verantwortliche meiner Behörde gegenüber rechenschaftspflichtig sind (Artikel 5 Absatz 2 DS-GVO). Können Arbeitgeberinnen und Arbeitgeber nicht belegen, dass eine Einwilligung freiwillig erteilt wurde, bleibt die Verarbeitung der Beschäftigtendaten rechtswidrig. In diesem Fall ergreife ich aufsichtsrechtliche Maßnahmen.

Zudem müssen Einwilligungen im Beschäftigtenverhältnis schriftlich erteilt werden und formellen Ansprüchen genügen (§26 Abs. 2 S. 3 und 4 BDSG).

J.7. Gesundheit und Soziales

7.1 Zweite anlassunabhängige Prüfung von 30 Krankenhäusern in Niedersachsen abgeschlossen

Wie in meinem 26. Tätigkeitsbericht angekündigt, habe ich die Prüfung der Umsetzung der Datenschutz-Grundverordnung (DS-GVO) in niedersächsischen Krankenhäusern in größerem Umfang fortgesetzt. Ziel war es, einen umfassenden Überblick über den Datenschutz zu erhalten und verbreitete Schwachstellen aufzudecken, um mit entsprechenden Abhilfemaßnahmen, reagieren zu können.

Ich verschickte einen Fragebogen mit insgesamt 15 Fragen zu den Teilgebieten Allgemeines Datenschutzrecht, Betroffenenrechte und Orientierungshilfe Krankenhausinformationssysteme. Die 30 geprüften Krankenhäuser entsprechen gut 20 Prozent der Krankenhäuser in Niedersachsen, somit kann von einem repräsentativen Ergebnis der Auswertung gesprochen werden.

Gut aufgestellt zu allgemeinen Fragen

Die Auswertung der Fragebögen ergab, dass die geprüften Krankenhäuser im Bereich der allgemeinen Fragen zum Datenschutz gut aufgestellt sind. Jede Einrichtung hat eine oder einen Datenschutzbeauftragten (DSB) benannt und alle Beschäftigten werden mindestens einmal jährlich datenschutzrechtlich geschult. Der Meldeweg für eine Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO ist ebenso in Verfahrensanweisungen festgelegt, wie der Ablauf einer Auskunft an die Betroffenen nach Art. 15 DS-GVO.

Datenschutzbeauftragte haben zu wenig Zeit für ihre Arbeit

DSB benötigt ausreichend Unterstützung

Die datenschutzrechtlichen Handlungsfelder in den Krankenhäusern sind vielfältig. Die betrieblichen Datenschutzbeauftragten vor Ort müssen die Einhaltung des Datenschutzes gegenüber den Beschäftigten genauso kontrollieren wie den Datenschutz in Bezug auf die Patientinnen und Patienten. Dies setzt nicht nur umfangreiche Kenntnisse im Datenschutzrecht voraus, sondern

auch ausreichende Zeitanteile bzw. eine ausreichende Anzahl an Beschäftigten, welche die oder den DSB, vertreten und unterstützen. Eine verspätete Meldung einer Datenpanne, nur weil die oder der DSB nicht erreichbar gewesen ist, wird von mir nicht toleriert.

Auch wenn die Datenschutzgesetze keine gesetzliche Pflicht zur Freistellung von Datenschutzbeauftragten vorsehen, sollte jedem Verantwortlichen bewusst sein, dass bereits in einem Krankenhaus mittlerer Größe mit mehreren Dutzend Beschäftigten und mehreren Tausend Patienten pro Jahr mindestens eine Vollzeitstelle pro Niederlassung für den Datenschutz eingeplant werden sollte.

Angesichts der, bei Verstößen gegen die DS-GVO drohenden Bußgelder, ist die Investition in ein zusätzliches Datenschutz-Team neben der oder dem kontrollierenden DSB nicht nur sinnvoll, sondern auch geboten.

Probleme beim Verzeichnis der Verarbeitungstätigkeiten

Alle Krankenhäuser gaben an, den gesetzlichen Vorgaben des Art. 30 DS-GVO zu entsprechen und über ein Verzeichnis der Verarbeitungstätigkeiten (VVT) zu verfügen. Den von mir angeforderten Auszug zu einer Verarbeitungstätigkeit legten einige Krankenhäuser jedoch nicht oder nicht vollständig vor. Diese Verantwortlichen werden im Rahmen eines nachgelagerten Kontrollverfahrens genauer überprüft.

Sorgfältig geführtes VVT schützt vor Verletzungen

Die gesetzliche Verpflichtung zur Führung eines VVT dient dazu, dass sich die Verantwortlichen über jede einzelne Verarbeitungstätigkeit Gedanken zum Schutz der personenbezogenen Daten machen. Unter Bezug auf die eingesetzten Mittel der Verarbeitung müssen sie eine Risikoanalyse durchführen und geeignete Maßnahmen ergreifen, um ein potenzielles Risiko zu minimieren oder bestenfalls auszuschließen. Ein sorgfältig geführtes VVT ist der beste Schutz vor einer Datenschutzverletzung.

Die Zahl der Einträge in den vorgelegten VVT reichte von 17 bis zu mehr als 800 Verarbeitungstätigkeiten. In kleineren Häusern mit weniger als 20.000 Patienten im Jahr lag der Durchschnitt bei 90 Verarbeitungstätigkeiten, in Häusern mit mehr als 20.000 Patienten im Jahr bei 207.

Datenschutzrechtlich ist es zulässig, gleichartige Verarbeitungsvorgänge mit denselben technisch-organisatorischen Schutzmaßnahmen in einem Eintrag im VVT zusammenzufassen. Zwar liegen mir keine Erkenntnisse vor, wie viele verschiedene Verarbeitungstätigkeiten in einem Krankenhaus tatsächlich vorhanden sind. Dennoch erscheint die vorliegende Spanne zu groß. Ich werde diesen Punkt daher im Jahr 2022 im Rahmen einer Nachprüfung gesondert betrachten.

Umsetzung der Betroffenenrechte

Patient/-innen haben Anspruch auf Kopie der Daten

Die Betroffenenrechte sind im medizinischen Bereich grundsätzlich nicht neu. Das Recht auf Einsicht in die Patientenakte wurde bereits 2013 im Patientenrechtegesetz[1] verankert. Mit Einführung des Art. 15 DS-GVO wurde den Betroffenen auch ein umfassender datenschutzrechtlicher

1 §§ 630a ff. BGB

Auskunftsanspruch sowie ein Anspruch auf eine kostenfreie Kopie der personenbezogenen Daten zugestanden. Erfreulich ist, dass es für die fristgemäße Umsetzung von Auskunftsersuchen in den geprüften Häusern entsprechende Verfahrensanweisungen gibt.

Bezüglich der Umsetzung der Betroffenenrechte nach den Artikeln 12 ff. DS-GVO ergaben sich keine Beanstandungen. Die allgemeinen Informationen zur Verarbeitung personenbezogener Daten sowie zum Beschwerderecht gem. Art. 13 DS-GVO werden allen Patientinnen und Patienten vor Beginn der Behandlung zugänglich gemacht.

Orientierungshilfe Krankenhausinformationssysteme

Die datenschutzrechtlichen Regelungen im Gesundheitswesen waren in Deutschland bereits vor der DS-GVO auf einem sehr hohen Niveau. Für den Bereich der Krankenhäuser gibt es seit fast zehn Jahren bereits eine von den Datenschutzaufsichtsbehörden entwickelte Orientierungshilfe Krankenhausinformationssysteme, welche die rechtlichen Auslegungen der Aufsichtsbehörden zu den Vorschriften zum Datenschutz formuliert. Diese Orientierungshilfe hat auch mit der DS-GVO ihre Gültigkeit behalten.

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

Wie auch bei der ersten Krankenhausprüfung festgestellt, gibt es bei der Umsetzung der OH KIS immer noch Verbesserungspotenzial. Eine regelmäßige Protokollierung und anlassunabhängige Auswertung der Zugriffe auf Patientenakten kann ebenso verbessert werden, wie die gem. Art. 18 DS-GVO vorgesehene Einschränkung der Verarbeitung abgeschlossener Fälle. Größere Beanstandungen ergab sich jedoch nicht.

Fazit der Prüfung

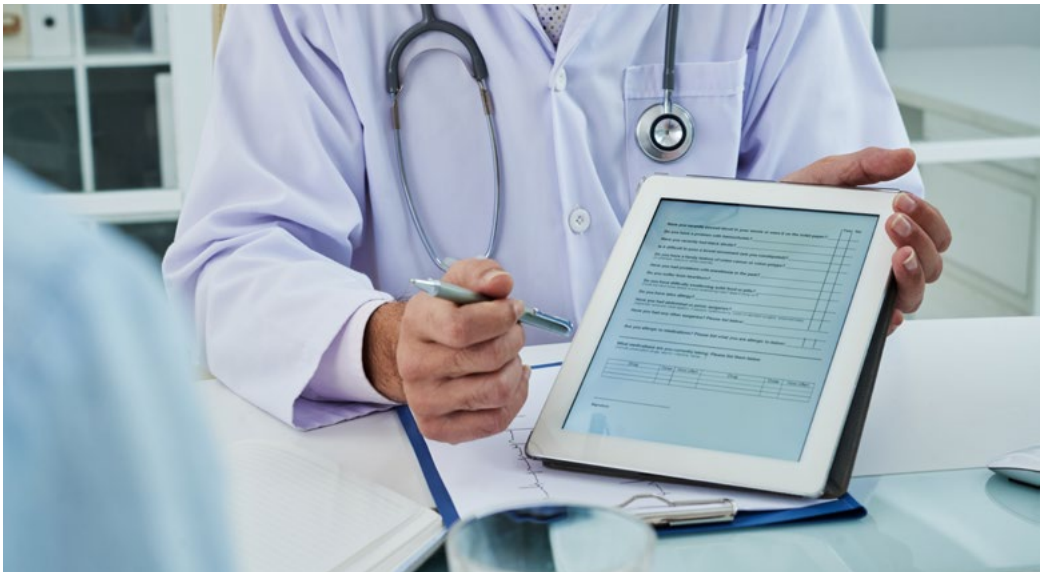
Die niedersächsischen Krankenhäuser sind – zum Teil mit Ausnahme des VVT – datenschutzrechtlich gut aufgestellt. Insgesamt gab es vier Krankenhäuser ohne jegliche Beanstandung und zehn Krankenhäuser mit nur jeweils einem kleinen Hinweis aufgrund uneindeutiger Formulierungen in den Stellungnahmen. In Anbetracht der Vielzahl an Fragen und dem strengen Prüfungsmaßstab ist dies ein sehr guter Wert.

Weiteres Vorgehen nach der Prüfung

Jedes geprüfte Krankenhaus erhielt einen individuellen Abschlussbericht. Die im Rahmen der Prüfung gestellten Fragen wurden von mir mit Darlegung meiner Rechtsauffassung beantwortet und allen Krankenhäusern in Form einer FAQ übersandt. Um diese Informationen allen Krankenhäusern in Niedersachsen zugänglich zu machen, habe ich die Niedersächsische Krankenhausgesellschaft gebeten, das Dokument ihren Mitgliedern zur Verfügung zu stellen.

Die gewonnenen Erkenntnisse werden zudem zeitnah in eine Ergänzung meiner allgemeinen FAQ im Gesundheitswesen eingearbeitet und auf meiner Webseite veröffentlicht.

7.2 Elektronische Patientenakte macht Fortschritte



In meinem Tätigkeitsbericht für 2020 habe ich ausführlich über ein Dilemma der gesetzlichen Krankenkassen berichtet: Aufgrund der fachgesetzlichen Vorgaben im Fünften Buch des Sozialgesetzbuchs konnten sie ihren Mitgliedern im Jahr 2021 nur eine elektronische Patientenakte mit einem datenschutzrechtlich unzureichenden Berechtigungskonzept zur Verfügung stellen.

Im Berichtszeitraum wurde der Umsetzungsstand des feingranularen Zugriffskonzepts der elektronischen Patientenakte bei der AOK Niedersachsen weiterverfolgt. Feingranular bedeutet, dass Patientinnen und Patienten im Detail entscheiden können, welche Behandler Zugriff auf welche Daten der Akte haben. 2021 war diese Eingrenzung zunächst nicht möglich, sodass Behandler entweder auf den gesamten Inhalt der Akte oder auf nichts zugreifen konnten.

Die AOK teilte mir mit, dass die Zusammenarbeit mit der gematik hinsichtlich der technischen Umsetzung zufriedenstellend funktioniere und man sich im Zeitplan befinde. Die gesetzlichen Vorgaben, zum 1. Januar 2022 eine elektronische Patientenakte mit einem datenschutzkonformen Berechtigungskonzept anbieten zu können, würden eingehalten.

Im Berichtszeitraum lagen mir keine Beschwerden von Bürgerinnen und Bürgern hinsichtlich der elektronischen Patientenakte vor. Laut Aussage der AOK Niedersachsen wurde diese in den ersten neun Monaten des Jahres 2021 jedoch auch nur von sehr wenigen Mitgliedern genutzt. Es bleibt abzuwarten, ob sich dies im Jahr 2022 ändert, wenn die elektronische Patientenakte mit dem feingranularen Berechtigungskonzept zur Verfügung steht.

7.3 Kontoauszüge für Bewegungsprofile im Sozialbereich

Wenn ein Sozialleistungsträger anzweifelt, dass eine Antragstellerin oder ein Antragsteller in seinem Zuständigkeitsbereich den gewöhnlichen Aufenthalt, darf er ihre oder seine Kontoauszüge in Bezug auf den Ort der Abhebungen auswerten.

In einem mir vorliegenden Fall ermittelte ein Sozialleistungsträger anhand der Kontoauszüge, die ihm eine antragstellende Person vorgelegt hatte, an welchen Orten diese Geld abgehoben hatte. Hierzu machte der Sozialleistungsträger die Standorte der Bankautomaten anhand deren Gerätenummern ausfindig.

Hintergrund für diese Ermittlung war, dass der Sozialleistungsträger berechtigte Zweifel daran hatte, dass die antragstellende Person in seinem Zuständigkeitsbereich ihren gewöhnlichen Aufenthalt hatte.

Die Rechtslage

Für den Sozialleistungsbereich bestimmt § 67 a Abs. 1 Satz 1 Zehntes Buch – Sozialgesetzbuch (SGB X), dass die Erhebung von Sozialdaten durch einen Sozialleistungsträger zulässig ist, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach dem Sozialgesetzbuch erforderlich ist. Die Kenntnis von Sozialdaten ist nur dann erforderlich, wenn sie notwendig ist, um die gesetzliche Aufgabe rechtmäßig, vollständig und in angemessener Zeit erfüllen zu können.[1]

Erforderlichkeit zur Erfüllung der gesetzlichen Aufgabe

Zu den Aufgaben, die einem Sozialleistungsträger nach dem Sozialgesetzbuch obliegen, gehört es z. B. berechtigte Sozialleistungen nach dem SGB II (Grundsicherung für Arbeitssuchende) zu gewähren.

Eine Nutzung von Sozialdaten durch einen Sozialleistungsträger ist zulässig[2], wenn die Vorschriften der §§ 67 b ff. SGB X oder eine andere Rechtsvorschrift des Sozialgesetzbuches dies erlauben oder anordnen. § 67 c Abs. 1 Satz 1 SGB X lässt die vorgenannte Nutzung zu, wenn sie zur Erfüllung der dem Sozialleistungsträger nach dem Sozialgesetzbuch obliegenden Aufgabe erforderlich ist und für diese Zwecke erfolgt.

1 BeckOK SozR/Westphal, 63. Ed. 01.12.2021, SGB X § 67 a Rn. 5
2 § 67 b Abs. 1 Satz 1 SGB X

Bei der Bearbeitung eines Antrages auf Gewährung von Sozialleistungen z. B. nach dem SGB II wird geprüft, ob der Sozialleistungsträger nicht nur sachlich[3], sondern auch örtlich für die Bearbeitung zuständig ist.

Gewöhnlicher Aufenthalt

Grundsätzlich örtlich zuständig ist ein zugelassener kommunaler Träger gemäß § 36 Abs. 1 Satz 2 SGB II, sofern die betroffene Person ihren gewöhnlichen Aufenthalt in dessen Gebiet hat. Seinen gewöhnlichen Aufenthalt hat jemand gemäß § 30 Abs. 3 Satz 2 SGB I dort, wo er sich unter Umständen aufhält, die erkennen lassen, dass er an diesem Ort oder in diesem Gebiet nicht nur vorübergehend verweilt.

Maßgebend für die Beurteilung eines gewöhnlichen Aufenthalts sind ein zeitliches Element („nicht nur vorübergehend"), der Wille der Person als subjektives Element und die objektiven Gegebenheiten („unter Umständen") mit einer vorausschauenden Betrachtung künftiger Entwicklungen, die eine gewisse Stetigkeit und Regelmäßigkeit des Aufenthalts erfordern.[4]

In diesem Fall war der Sozialleistungsträger als zugelassener kommunaler Träger sachlich zuständig. Dessen örtliche Zuständigkeit war zum Zeitpunkt der Antragstellung aufgrund der Angaben der betroffenen Person auch zunächst anzunehmen.

Zweifel am tatsächlichen Aufenthalt

Im Rahmen der sich anschließenden Prüfung der Anspruchsvoraussetzungen für eine Leistung zur Grundsicherung hatte der Sozialleistungsträger von der betroffenen Person u. a. Kontoauszüge eingefordert. Diese Datenerhebung ist im Hinblick darauf, dass die betroffene Person ihre Hilfebedürftigkeit nachzuweisen hat, gemäß § 67 a Abs. 1 Satz 1 SGB X rechtmäßig.[5]

Im weiteren Verfahren kamen dem Sozialleistungsträger bei näherer Prüfung der ihm von der betroffenen Person vorgelegten Unterlagen[6], Zweifel daran, dass deren Angaben zu ihrem gewöhnlichen Aufenthalt den Tatsachen entsprachen.

Untersuchungsgrundsatz

3 Sachlich zuständig sind z. B. die zugelassenen kommunalen Träger (§ 6 a SGB II in Verbindung mit der Verordnung zur Zulassung von kommunalen Trägern als Träger der Grundsicherung für Arbeitsuchende).
4 BeckOK SozR/Mushoff, 63. Ed. 01.12.2021, SGB II § 7 Rn. 17
5 s. Entscheidung des Bundessozialgerichts - BSG, Urteil vom 19.09.2008 - B 14 AS 45/07 R
6 hier: Vorlage Personalausweis nebst Kopie einer Meldebescheinigung

Daher hatte der Sozialleistungsträger im Rahmen des auch im SGB II geltenden Untersuchungsgrundsatzes die Sachlage von Amts wegen zu ermitteln. Hierbei bestimmt der Sozialleistungsträger gemäß § 20 Abs. 1 Satz 2 SGB X die Art und den Umfang der Ermittlungen. Allerdings muss sich der Sozialleistungsträger bei der Ermittlung auf die für die Entscheidung notwendigen Sachfragen beschränken.

Beweismittel müssen verhältnis- und zweckmäßig sein

Zur Ermittlung des Sachverhalts darf sich der Sozialleistungsträger der Beweismittel bedienen, die er nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält (§ 21 Abs. 1 Satz 1 SGB X). Es gibt keine Beschränkung hinsichtlich möglicher Beweismittel. Allerdings sind entsprechend dem Amtsermittlungsprinzip bei der Auswahl der Beweismittel die Grundsätze der Verhältnismäßigkeit und Zweckmäßigkeit zu beachten.[7]

Im vorliegenden Fall hatte der Sozialleistungsträger anhand der ermittelten Standorte der Bankautomaten festgestellt, dass die Kontoabhebungen ausschließlich an Bankautomaten außerhalb des Gebietes erfolgt waren, für das er örtlich zuständig ist.

Die Ermittlung, an welchen Standorten Kontoabhebungen erfolgen, ist ein geeignetes Mittel, um darauf schließen zu können, wo eine betroffene Person ihren gewöhnlichen Aufenthalt gemäß § 30 Abs. 3 Satz 2 SGB I hat.

Die Ermittlung war auch erforderlich, da im vorliegenden Fall die betroffene Person selbst keine für den Sozialleistungsträger nachvollziehbare und tragfähige Erklärung zu ihrem gewöhnlichen Aufenthalt vorgetragen hatte. Ferner erfolgte die Ermittlung auch nur, um aufzuklären, ob die betroffene Person tatsächlich ihren gewöhnlichen Aufenthaltsort im Zuständigkeitsbereich des Sozialleistungsträgers hatte.

Im vorliegenden Fall durfte der Sozialleistungsträgers also die aus den Kontoauszügen ersichtlichen Daten für die Erstellung eines Bewegungsprofils der betroffenen Person gemäß § 67 c Abs. 1 Satz 1 SGB X nutzen.

7 BeckOK SozR/Weber, 63. Ed. 01.12.2021, SGB X § 21 Rn. 3

7.4 Umfang des Auskunftsrechts im Sozialbereich

Im Gegensatz zum allgemeinen Recht wird das Auskunftsrecht gem. Art. 15 Datenschutz-Grundverordnung (DS-GVO) im Sozialrecht durch die Regelungen des § 83 Abs. 2 Sozialgesetzbuch – Zehntes Buch (SGB X) eingeschränkt und an die Mitwirkung der Betroffenen gekoppelt.

Wie in allen anderen Rechtsbereichen liegen mir auch im Sozialrecht immer wieder Beschwerden von Betroffenen zum Auskunftsrecht vor. Oftmals ist den Betroffenen nicht bekannt, dass sie im Sozialrecht bei Beantragung einer Auskunft über die zu ihrer Person verarbeiteten Daten einer Mitwirkungspflicht unterliegen.

Zum Schutz der sozialen Sicherheit hat der Gesetzgeber im Sozialbereich mit § 83 Abs. 2 SGB X von der Öffnungsklausel des Art. 23 Abs. 1 lit. e in Verbindung mit Abs. 2 lit. c und g DS-GVO Gebrauch gemacht[1]. Die Beschränkung des Auskunftsrechts durch die Normierung von Mitwirkungspflichten soll die verantwortlichen Stellen vor unverhältnismäßiger Inanspruchnahme schützen, damit diese ihrem gesetzlichen Auftrag der sozialen Sicherung nachkommen können.

> § 83 Abs. 2 SGB X
> Die betroffene Person soll in dem Antrag auf Auskunft gemäß Artikel 15 der Verordnung (EU) 2016/679 die Art der Sozialdaten, über die Auskunft erteilt werden soll, näher bezeichnen. Sind die Sozialdaten nicht automatisiert oder nicht in nicht automatisierten Dateisystemen gespeichert, wird die Auskunft nur erteilt, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Soweit Artikel 15 und 12 Absatz 3 der Verordnung (EU) 2016/679 keine Regelungen enthalten, bestimmt der Verantwortliche das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. § 25 Absatz 2 gilt entsprechend.

Betroffene müssen Angaben zum Auffinden der Daten machen

Die Betroffenen haben demnach Angaben zum Auffinden der Daten (beispielsweise das Aktenzeichen) sowie zu dem jeweiligen Aktenvorgang (beispielsweise: „Welche Informationen wurden im Zeitraum XY an Dritte weitergegeben“) zu machen.

1 (BT-Drs. 18/12611, 120)

Enthält der Antrag auf Auskunft keine konkretisierenden Angaben, hat der Verantwortliche die Betroffenen aufzufordern, diese Angaben nachzuholen. Werden von den Betroffenen weiterhin keine entsprechenden Angaben gemacht, hat der Verantwortliche zu prüfen, ob eine Auskunft erteilt werden kann oder ob das Auskunftsersuchen abzulehnen ist. Die Gründe für eine Ablehnung sind zu dokumentieren (§ 83 Abs. 3 SGB X).

Verantwortlicher bestimmt Form der Auskunft

Wird ein Auskunftsersuchen bewilligt, bestimmt der Verantwortliche das Verfahren, insbesondere die Form, in der die Auskunft erteilt wird, nach pflichtgemäßem Ermessen. Sofern den Betroffenen beispielsweise aufgrund des Umfangs einer Akte und der Vielzahl an Daten angeboten wird, das Auskunftsersuchen durch Akteneinsicht zu erfüllen, müssen im Rahmen der Akteneinsicht auf Wunsch unentgeltlich Kopien zu den von den Betroffenen vor Ort genannten personenbezogenen Daten gefertigt werden.

J.8. Telemedien

8.1 TTDSG: Wirksames Werkzeug gegen rechtswidriges Tracking

Kurz vor Jahresende 2021 ist am 1. Dezember das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) in Kraft getreten. Das TTDSG ist ein bereichsspezifisches nationales Datenschutzgesetz, in dem die wesentlichen Datenschutzvorschriften für Telekommunikations- und Telemediendienste zusammengefasst worden sind. Die in Literatur und Praxis wohl am meisten diskutierte Vorschrift ist der § 25 TTDSG. Mit diesem wird mit zwölf Jahren Verzögerung endlich die sogenannte Cookie-Regelung der europäischen ePrivacy-Richtlinie europarechtskonform in nationales Recht umgesetzt.

Anlass der Gesetzgebung war die europäische Richtlinie (2018/1972/EU) über den europäischen Kodex für die elektronische Kommunikation, die eine Änderung des Telekommunikationsgesetzes (TKG) erforderlich machte. Der Gesetzgeber nahm dabei die Gelegenheit wahr, die bisher nicht an die DS-GVO angepassten Datenschutzvorschriften des TKG und des Telemediengesetzes (TMG) im neuen TTDSG zusammenzuführen. Ziel war es, beide Bereiche an die DS-GVO und die E-Privacy-Richtlinie anzupassen und insbesondere die Vorgaben aus Art. 5 Abs. 3 der E-Privacy-Richtlinie – die bereits seit 2009 gelten – rechtssicher in nationales Recht umzusetzen. Danach dürfen grundsätzlich Informationen auf Endgeräten nur gespeichert oder von diesen ausgelesen werden, wenn der Nutzer vorher eingewilligt hat.

Nach den ursprünglichen Plänen der Europäischen Kommission sollte zeitgleich mit der DS-GVO eine europäische Verordnung über Privatsphäre und elektronische Kommunikation (die E-Privacy-Verordnung) in Kraft treten und die Richtlinie ersetzen. Selbst Anfang 2022 war jedoch noch immer nicht absehbar, ob und wann es eine solche E-Privacy-Verordnung geben wird. Sollte es dazu kommen, würde das TTDSG weitgehend von der Verordnung als höherrangigem Recht mit unmittelbarer Wirkung in den Mitgliedstaaten abgelöst werden.

Neues Gesetz vereinfacht die Rechtsanwendung

Die Zusammenführung der Datenschutzvorschriften des TKG und des TMG vereinfacht die Rechtsanwendung und sorgt für Rechtsklarheit. Da Telekommunikations- und Telemediendienste in einem sehr engen sachlichen Zusammenhang stehen – Telemediendienste basieren technisch auf Telekommunikationsdiensten – ergänzt das TTDSG bereichsspezifisch für öffentliche und nicht öffentliche Stellen einheitlich die DS-GVO. Es sind somit grundsätzlich diese beiden Gesetze bei einer datenschutzrechtlichen Bewertung von Telekommunikations- und Telemediendiensten zu prüfen.

Mit dem TTDSG werden die Datenschutzvorschriften für Telekommunikation und Telemedien ebenfalls mit mehr als zweijähriger Verzögerung an die DS-GVO angepasst. Dadurch entfallen die bisher schwierigen Abgrenzungs- und Anwendungsprobleme im Verhältnis zwischen den bis zum TTDSG gelten spezifischen nationalen Datenschutzvorschriften im TMG und der europäischen DS-GVO. Die Anpassung erschöpft sich allerdings weitgehend darin, dass Datenschutzvorschriften, für die in der DS-GVO keine Öffnungsklausel bestehen, nicht in das TTDSG übernommen worden sind, wie insbesondere die Rechtsgrundlagen für die Verarbeitung von Bestands- und Nutzungsdaten bei Telemedien.

Neudefinition für Telekommunikationsdienste

Durch die Umsetzung des Europäischen Kodex für elektronische Kommunikation im neuen Telekommunikationsgesetz ist die Definition für Telekommunikationsdienste in § 3 Nr. 61 TKG neu gefasst worden. Sie umfasst nun ausdrücklich die interpersonellen Telekommunikationsdienste, zu denen Internettelefonie (Voice-Over-IP), webgestützte E-Mail- und mobile Instant-Messenger-Dienste gehören. In der Gesetzesbegründung wird hierzu zutreffend ausgeführt, dass diese Online-Dienste aus der Perspektive des Endnutzers in der Funktionalität den klassischen Telekommunikationsdiensten gleichwertig sind. Es ist sehr erfreulich, dass klargestellt ist, dass Anbieter von öffentlich zugänglichen Diensten zur interpersonellen Kommunikation umfassend zur Wahrung des Fernmeldegeheimnisses verpflichtet sind.

Zur bisherigen Rechtslage in Bezug auf E-Mail-Dienste, siehe S. 48 ff des Tätigkeitsberichts 2019: https://t1p.de/TB2019

Darüber hinaus sieht das TTDSG für Anbieter von öffentlichen Telekommunikationsdiensten in den spezifischen Datenschutzvorschriften (§§ 3 bis 18) nicht allzu viele Änderungen im Vergleich zur vorherigen Rechtslage vor. Aufgrund der aufsichtsbehördlichen Sonderzuständigkeit des BfDI für Telekommunikationsdienstleister hatte meine Behörde in der Vergangenheit kaum Berührung mit den spezifischen Datenschutzvorschriften im TKG und dies wird auch zukünftig so sein.

Für Telemedien finden sich im TTDSG in den §§ 19 bis 24 nur wenige Datenschutzvorschriften. Es enthält im Unterschied zum bisher geltenden TMG keine spezifischen Erlaubnistatbestände für Bestands- und Nutzungsdaten bei Telemedien (§§ 14 und 15 TMG a.F.), sodass allein Art. 6 und Art. 9 DS-GVO für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten maßgeblich sind. Ich begrüße das, da die Differenzierung zwischen personenbezogenen Bestands- und Nutzungsdaten einerseits und sogenannten Inhaltsdaten, die nach den allgemeinen Datenschutzvorschriften zu bewerten waren, andererseits kaum noch praktikabel und sinnvoll war. Es gibt auch

keine Sonderregelung für die elektronische Einwilligung mehr (ehemals § 13 Abs. 2 und 3 TMG), sodass allein die Vorschriften der DS-GVO maßgeblich sind.

Tracking nur mit Einwilligung

Eine – zumindest im nationalen Recht – neue Vorschrift ist § 25 TTDSG, der sehr relevant für die Praxis ist. Demnach bedürfen das Speichern von Informationen in Endeinrichtungen und der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, der Einwilligung des Nutzers oder der Nutzerin. Anwendbar ist die Vorschrift insbesondere für Cookies und andere Tracking-Methoden, die verwendet werden, um Nutzerinnen und Nutzer von Webseiten und Apps wiederzuerkennen und zu identifizieren. Mit ihrer Hilfe wird z. B. das Surfverhalten auf der Webseite ausgewertet, um diese zu optimieren, oder es werden Profile über die Vorlieben und Interessen der Nutzerinnen und Nutzer erstellt, um ihnen individualisierte Werbeanzeigen auf der Webseite auszuspielen. Hierbei werden anschließend personenbezogene Daten verarbeitet. Diese nachgelagerten Verarbeitungen fallen nicht in den Anwendungsbereich von § 25 TTDSG; sie sind uneingeschränkt nach der DS-GVO zu beurteilen.

FAQ zum TTDSG:
https://t1p.de/FAQ-TTDSG

Es gibt zwar Ausnahmen von diesem grundsätzlichen Einwilligungserfordernis, allerdings sind diese sehr begrenzt. Auf eine Einwilligung kann verzichtet werden, wenn der Einsatz der Cookies oder die Einbindung von Drittdiensten unbedingt erforderlich sind, damit Anbieter einen vom Nutzer oder von der Nutzerin ausdrücklich gewünschten Telemediendienst zur Verfügung stellen können. Solche Drittdienste auf Webseiten sind beispielweise Consent-Management-Tools, Analysedienste zur Reichweitenmessung und Webseitenoptimierung, Videoplattformen, Chat-Dienste, Karten- oder Bezahldienste. Es gibt eigentlich kaum Webseiten, auf denen keine Cookies gesetzt werden und bei denen keine Drittdienste eingebunden sind.

Orientierungshilfe für Anbieter von Telemedien:
https://t1p.de/OH-Telemedien

Insgesamt führt das TTDSG nach meiner Einschätzung bei einigen wichtigen Fragen zu einer Klarstellung und damit zu deutlich mehr Rechtssicherheit. Mit dem § 25 TTDSG haben die deutschen Aufsichtsbehörden nun endlich eine eindeutige Vorschrift, um effektiv gegen die vielfach rechtswidrigen Praktiken des Trackings auf Webseiten und in Apps vorgehen zu können. Wie nahezu jedes neues Gesetz führt das TTDSG aber auch zu neuen und interessengesteuerten Diskussionen, wie einzelne Vorschriften konkret anzuwenden und auszulegen sind. Als Unterstützung für alle, die das TTDSG beachten müssen, habe ich auf meiner Webseite FAQs zur Verfügung gestellt, um grundlegende Fragen zum TTDSG zu beantworten. Darüber hinaus freue mich besonders, dass die Datenschutzkonferenz sich mit der neuen Orientierungshilfe für Anbieter von Telemedien bereits frühzeitig zu wesentlichen Anwendungs- und Auslegungsfragen positioniert hat und praktische Hilfestellung bietet.

8.2 Länderübergreifende Prüfung der Webseiten von Medienunternehmen – Einwilligungen meist unwirksam

Die Datenschutzaufsichtsbehörden mehrerer deutscher Länder haben unter meiner Koordination die Webseiten von Medienunternehmen auf den Einsatz von Cookies und die Einbindung von Drittdiensten untersucht. Insgesamt wurden auf Basis eines gemeinsamen Prüfkatalogs 49 Webangebote in 11 Bundesländern geprüft. Schwerpunkt war das Nutzertracking zu Werbezwecken. Die meisten der geprüften Webseiten entsprechen nicht den rechtlichen Anforderungen für den Einsatz von Cookies und anderen Trackingtechniken. Die Medienunternehmen verstoßen damit gegen das Recht ihrer Nutzerinnen und Nutzer auf Schutz ihrer personenbezogenen Daten. Auch erste Anpassungen bei einigen Verantwortlichen konnten die rechtlichen Defizite bisher nicht vollständig beseitigen.

Fragen zu Drittanbietern und Cookies

Für die koordinierte Prüfung verschickten die Behörden aus Baden-Württemberg, Brandenburg, Bremen, Hamburg, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, dem Saarland, Sachsen und Schleswig-Holstein einen gemeinsam erarbeiteten Fragebogen an Medienunternehmen in ihren jeweiligen Zuständigkeitsbereichen. Die Unternehmen sollten unter anderem beantworten, ob sie Dienste von Drittanbietern (z. B. Karten- oder Wetterdienste) eingebunden hatten, ob sie Cookies einsetzen und ob sie deren Verwendung auf eine Einwilligung der Nutzerinnen und Nutzer stützen. Es wurden umfangreiche und detaillierte Tabellen zu den eingesetzten Cookies und Drittdiensten angefordert. Geprüft wurden nicht sämtliche Webseiten der Unternehmen, sondern deren reichweitenstärkste Angebote.

In Niedersachsen wurden fünf Medienhäuser jeweils zu einer konkreten Webseite kontaktiert. Bereits vor dem Versand der Fragebögen waren die ausgewählten Webseiten technisch gesichert und analysiert worden. So war ein Abgleich zwischen den Antworten der Medienunternehmen und der tatsächlichen technischen Gestaltung der Seiten möglich. Für die rechtliche Bewertung wurde eine erneute technische Prüfung vorgenommen. Neben den bereits genannten Stellen beteiligte sich auch die Aufsichtsbehörde in Bayern an der inhaltlichen Auswertung der Untersuchungsergebnisse.

Grundlagen der Auswertung waren die ausgefüllten Fragenbögen, die Ergebnisse der technischen Prüfungen der Webseiten sowie die auf den Webseiten integrierten Einwilligungsbanner und verfügbaren Datenschutzerklärungen.

Kriterien für die Bewertung

Im Einzelnen wurden die folgenden Kriterien bewertet:

1. Rechtmäßigkeit der Datenverarbeitung im Zusammenhang mit lokalen Speicherobjekten, Tracking-Techniken und Drittdiensten
2. Wirksamkeit der Einwilligung, sofern eine Einwilligung auf der Website für die Verarbeitung von lokalen Speicherobjekten, Tracking-Techniken und Drittdiensten eingeholt wird
3. Erfüllung der Informationspflichten gemäß Art. 13 DS-GVO
4. Umsetzung datenschutzfreundlicher Voreinstellungen gemäß Art. 25 Abs. 2 DS-GVO
5. Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO
6. Erfüllung der Nachweispflichten gemäß Art. 5 Abs. 2 DS-GVO.

Der Schwerpunkt der datenschutzrechtlichen Bewertung lag auf den ersten drei Aspekten und beruhte auf zwischen den beteiligten Behörden abgestimmten Bewertungsmaßstäben. Die niedersächsischen Unternehmen erhielten im September 2021 Auswertungsschreiben, in denen detaillierte Hinweise erteilt wurden. Den Verantwortlichen bekamen zudem die Gelegenheit zur Stellungnahme zu den festgestellten Datenschutzverstößen. Die abschließende Entscheidung, ob ich aufsichtsbehördliche Maßnahmen ergreifen muss, steht noch aus. Zeitnah nach der Versendung der Prüfanschreiben wurden auf den geprüften Webseiten Anpassungen in unterschiedlichen Umfang vorgenommen.

Wesentliche Ergebnisse

Bis zu 2.300 Drittdienste auf einer Webseite

Meine Vermutung, dass auf den geprüften Medienwebseiten eine sehr hohe Anzahl von Cookies und Drittdiensten verwendet wird, hat sich bestätigt. Der Höchstwert in Niedersachsen: Auf einer einzelnen Webseite wurden über den eingebundenen Einwilligungsbanner für mehr als 2.300 Drittdienste Einwilligungen der Nutzerinnen und Nutzer abgefragt. Nur ein sehr geringer Anteil der Drittdienste und Cookies war für die Funktionsfähigkeit der Webseite erforderlich. Sie dienten überwiegend dem Nutzertracking und der Finanzierung durch Werbung.

Für Nutzerinnen und Nutzer besteht durch diese Praxis der Medienunternehmen ein erhebliches Risiko. Die im Rahmen des Nutzertrackings erhobenen personenbezogenen Daten werden insbesondere zur Erstellung und Anreicherung umfassender und seitenübergreifender Persönlichkeitsprofile genutzt. Diese werden für das Online-Marketing, vor allem im Real Time Bidding-Verfahren (Echtzeitauktion von Werbeplätzen) eingesetzt.

Die Webseiten fragten zwar in der Regel differenzierte Einwilligungen der Nutzerinnen und Nutzer für die Verwendung von Cookies und Drittdiensten ab. In der Mehrheit der Fälle waren diese Einwilligungen allerdings nicht wirksam.

Häufig festgestellte Mängel

Im Rahmen der Prüfung wurden vor allem die folgenden Mängel festgestellt:

- Falsche Reihenfolge: Häufig wurden einwilligungsbedürftige Drittdienste bereits beim Öffnen der Webseiten eingebunden und Cookies gesetzt – also noch vor der Einwilligungsabfrage.
- Fehlende Informationen: Auf der ersten Ebene der Einwilligungsbanner wurden nur unzureichende oder falsche Informationen über das Nutzertracking gegeben.
- Unzureichender Einwilligungsumfang: Selbst wenn Nutzerinnen und Nutzer die Möglichkeit wahrnahmen, bereits auf der ersten Ebene des Einwilligungsbanners alles abzulehnen, blieben zahlreiche Cookies und Drittdienste aktiv, die eine Einwilligung erfordern.
- Keine einfache Ablehnung: Während bei allen Einwilligungsbannern auf der ersten Ebene eine Schaltfläche vorhanden war, mit der eine Zustimmung zu sämtlichen Cookies und Drittdiensten erteilt werden konnte, fehlte auf dieser Ebene häufig eine ebenso einfache Möglichkeit, das einwilligungsbedürftige Nutzertracking in Gänze abzulehnen oder das Banner ohne Entscheidung schließen zu können.
- Manipulation der Nutzerinnen und Nutzer: Die Ausgestaltung der Einwilligungsbanner wies zahlreiche Formen des Nudging auf. Das bedeutet, Nutzerinnen und Nutzer werden unterschwellig zur Abgabe einer Einwilligung gedrängt, indem die Schaltfläche für die Zustimmung beispielsweise durch eine farbliche Hervorhebung deutlich auffälliger gestaltet ist als die Schaltfläche zum Ablehnen oder indem die Verweigerung der Einwilligung unnötig verkompliziert wird.

Aufgrund der neuen Rechtslage durch die Geltung des TTDSG ab dem 1. Dezember 2021 konnte die Prüfung im vergangenen Jahr nicht vollständig abgeschlossen werden. Das TTDSG ist für die rechtliche Bewertung des Prüfgegenstandes sehr relevant, so dass diese angepasst werden muss, auch wenn sich im Ergebnis letztlich keine wesentlichen Unterschiede ergeben werden.

Fazit

Die koordinierte Prüfung hat erstens sehr deutlich gezeigt, wie intensiv das Nutzertracking auf Webseiten von Medienunternehmen eingesetzt wird und in welchem Ausmaß es dadurch zu Datenschutzverstößen auf diesen Webseiten kommt. Vermutlich gilt diese Feststellung auch für zahlreiche andere werbefinanzierte Webseiten, auf denen werthaltiger Content oder Dienstleistungen angeboten werden, ohne dass Nutzerinnen und Nutzer ein Entgelt dafür zahlen. Darüber hinaus habe ich die Erkenntnis gewonnen, dass der koordinierte länderübergreifende Ansatz der Medienprüfung den Datenschutz in der Praxis auch über die konkret geprüften Unternehmen hinaus deutlich verbessert. Ein solches gemeinsames Vorgehen ist zwar aufgrund der erforderlichen Abstimmungsprozesse der Aufsichtsbehörden untereinander aufwändig, erzeugt aber eine große Breitenwirkung.

8.3 Sicherheitslücken in „Microsoft Exchange Servern“

In der Nacht auf den 3. März 2021 gab Microsoft vier sicherheitsrelevante Schwachstellen in seiner Software „Microsoft Exchange Server“ bekannt. Gleichzeitig wurden Patches von Microsoft bereitgestellt, um die Sicherheitslücken zu schließen. Automatisierte Suchen im Internet nach anfälligen Servern und Angriffe auf die entsprechende IT-Infrastruktur begannen unmittelbar nach der Veröffentlichung. Für meine Behörde hatte dieser Vorfall zahlreiche Meldungen von Datenschutzverletzungen zur Folge.

Am 5. März 2021 gab das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Sicherheitsmeldung bezüglich der vier Schwachstellen heraus und stufte die Bedrohungslage als extrem kritisch (Stufe 4, Rot) ein. Es sah die Server einem sehr hohen Angriffsrisiko ausgesetzt und empfahl dringend, die Patches sofort einzuspielen sowie die Systeme auf Auffälligkeiten zu überprüfen.

Verletzung des Datenschutzes durch Sicherheitslücken

Die unter dem Namen „ProxyLogon“ oder auch „Hafnium Hack“ bekannt gewordenen Schwachstellen erlauben es Angreifenden, auch ohne Zugangsdaten, Mails von beliebigen Postfächern auszulesen, beliebige Dateien auf dem Exchange-Server zu schreiben und eigene Codes auf dem Exchange-Server im Kontext des System-Benutzers auszuführen.[1] Dies schloss das Auslesen von Adressbüchern ein und eröffnete z. B. die Möglichkeit, sogenannte Ransomware mit erpresserischer Absicht zu installieren.

Auslesen von Adressbüchern möglich

Da E-Mails und Adressbücher somit – zumindest bei einer Ausnutzung der Schwachstellen – einem unbefugten Zugang ausgesetzt waren, führten die Schwachstellen zu einer Verletzung des Schutzes von personenbezogenen Daten.

Hinweise für Verantwortliche: https://t1p.de/ms-exchange

Das BSI betonte, dass bei Systemen, die bis dato nicht gepatched worden waren, von einer Kompromittierung ausgegangen werden sollte. Zur Begründung verwies das Amt auf die öffentliche Verfügbarkeit von sogenannten Proof-of-Concept Exploit-Codes sowie die starken weltweiten Scan-Aktivitäten.

1 vgl. Bundesamt für Sicherheit in der Informationstechnik: Microsoft Exchange Schwachstellen CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065 Detektion und Reaktion Version 2.4, Stand 19.03.2021

Meinerseits informierte ich auf meiner Webseite darüber, dass in jedem Fall einer Kompromittierung des Exchange Servers sowie eines nicht rechtzeitigen Updates eine Meldung gemäß Art. 33 DS-GVO abzugeben sei. Eine Ausnahme von dieser Grundregel galt für Verantwortliche, die bereits nach den Handlungsempfehlungen des BSI geprüft hatten, ob die Sicherheitslücke ausgenutzt worden war und keine Kompromittierung festgestellt hatten. Diese konnten von einer Meldung absehen, da in diesem Fall voraussichtlich kein Risiko für die Rechte und Freiheiten der betroffenen Personen vorlag. In jedem Fall war hingegen die Dokumentation nach Art. 33 Abs. 5 DS-GVO zu erstellen.

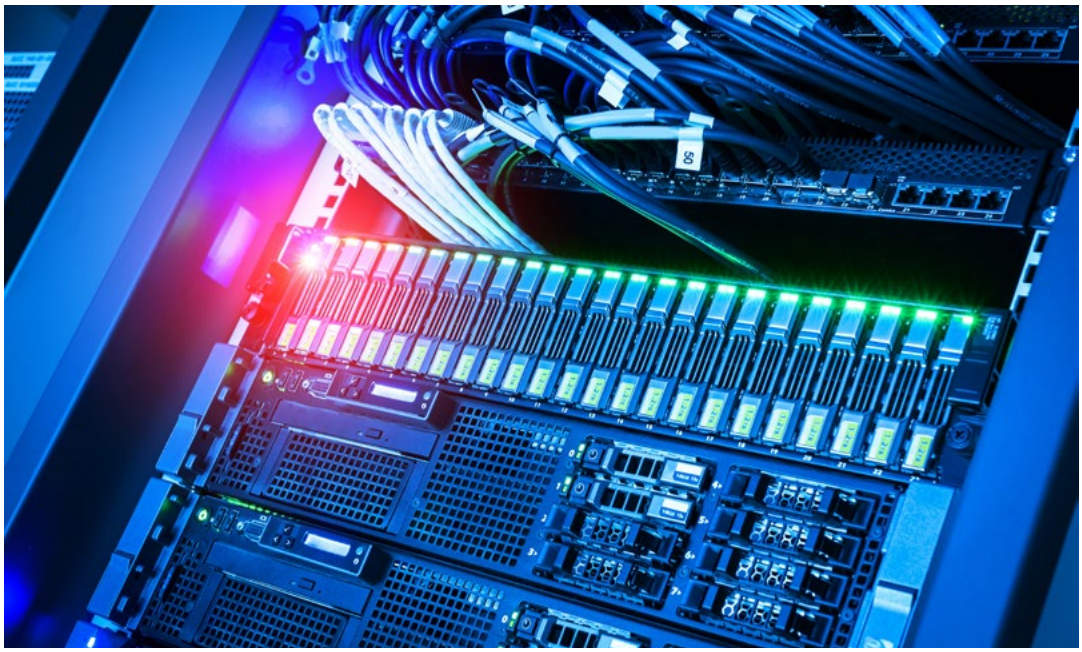
500 Meldungen nach Art. 33 DS-GVO

Nach der Pressemitteilung des BSI gingen knapp 500 Meldungen einer Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO bei mir ein. Davon entfielen rund 80 Prozent auf nicht öffentliche und rund 20 Prozent auf öffentliche Stellen. Höhepunkt der Eingangszahlen waren die Tage vom 9. bis 12. März 2021.

Zunächst Prüfung auf Auffälligkeiten

Um die Gefährdung der Sicherheit der personenbezogenen Daten und damit die Datenschutzverletzungen möglichst zeitnah zu beenden, wurden die Meldungen auf die Schilderung von Auffälligkeiten geprüft. Mit der von meiner Behörde verschickten Eingangsbestätigung wurde auf die laufend aktualisierten Empfehlungen des BSI und die Informationen auf meiner Homepage hingewiesen. Ferner gab ich Hinweise zur Dokumentation des Vorfalls und auf die eventuell bestehende Pflicht zur Information der Betroffenen.

Im nächsten Schritt wurden alle Meldungen einer Einzelprüfung unterzogen. Ein Hauptkriterium war dabei, ob sich aus der vorliegenden Meldung ergab, dass der Verantwortliche bereits zeit-



nah ausreichende Maßnahmen zur Schließung der Schwachstelle und damit zur Beendigung der Schutzverletzung ergriffen hatte. Bei rund einem Drittel der Meldungen waren nicht genügend Informationen mitgeteilt worden, sodass bei den Verantwortlichen ergänzende Informationen angefordert werden mussten. Um die Meldenden zu unterstützen und das Verfahren zielgerichtet fortzuführen, wurde dazu ein Fragebogen an die betroffenen Stellen verschickt. Anhand der Rückläufe wurde deutlich, dass in den allermeisten Fällen die Verantwortlichen die erforderlichen Maßnahmen zur Schließung der Schwachstelle ergriffen, ihr System auf Kompromittierung untersucht und ggf. bereinigt hatten. Im Einzelfall waren von mir weitere gezielte Nachfragen nötig, damit letztlich alle Verantwortlichen die Empfehlungen des BSI umsetzten.

Viele Verantwortliche hatten schnell gehandelt

Bei über der Hälfte der im März und April eingegangenen Meldungen zeigte sich erfreulicherweise, dass die Verantwortlichen bereits zügig angemessene Maßnahmen umgesetzt hatten. Ein Teil der Verantwortlichen hatte jedoch verspätet gemeldet, also nach Ablauf der Regelfrist von 72-Stunden aus Art. 33 Abs. 1 DS-GVO. Diese Verantwortlichen wurden darauf hingewiesen, dass die 72-Stunden-Frist ab Bekanntwerden der Sicherheitslücke zu laufen begann und nicht erst ab der Information durch (externe) IT-Dienstleister, welche die Verantwortlichen oft erst nach Abschluss ihrer Tätigkeiten informiert hatten.

Zahlreiche Angriffe aber wenige Datenzugriffe

Die Untersuchungen durch die Verantwortlichen ergaben, dass in den meisten der gemeldeten Fälle die Schwachstellen bis zu deren Schließung noch nicht intensiv ausgenutzt worden waren. Dies entspricht dem zeitlichen Ablauf typischer Angriffsszenarien mit einem stufenweisen Vorgehen. Es konnten in den allermeisten Fällen Angriffsspuren und häufig bereits die Installation einer sogenannten Webshell festgestellt werden. Das ist eine Schnittstelle, die den Fernzugriff auf einen Webserver, häufig speziell für einen Cyberangriff, ermöglicht. Jedoch war in der weit überwiegenden Zahl der Fälle noch keine weitere Schadsoftware installiert worden und es waren keine Spuren für einen umfangreichen Export von personenbezogenen Daten entdeckt worden.

Datenzugriff in Einzelfällen nachweisbar

In Einzelfällen war ein Zugriff auf personenbezogene Daten nachweisbar. Dieser betraf in der Regel die Outlook Offline-Adressbücher, die gelöscht oder heruntergeladen worden waren. Diese enthielten jeweils nur wenige personenbezogene Daten aus niedrigen Schutzstufen. Sehr vereinzelt wurden weitergehende Ausnutzungen der Schwachstellen bekannt. Dabei fanden mit einigem zeitlichen Versatz Angriffe mit Ransomware statt. Mitunter wurde eine Bitcoin Mining Software installiert.

Schwachstellen ohne Verteidigungsmöglichkeit

Den Angriffen lag ein Zero-Day-Exploit, also bis dahin im Wesentlichen unbekannte Schwachstellen, zugrunde. Es bestand für die Verantwortlichen keine Möglichkeit, die Ausnutzung der Schwachstellen vor deren Veröffentlichung zu verhindern. Aus diesem Grund habe ich in diesen Fällen von aufsichtsbehördlichen Maßnahmen abgesehen, wenn zeitnah die erforderlichen Maßnahmen ergriffen worden waren, wie dies zumeist der Fall war.

In meinem Abschlussschreiben gab ich den betroffenen Stellen noch einmal weitere Hinweise zu sinnvollen zusätzlichen Maßnahmen für den Datenschutz und die IT-Sicherheit.

J.9. Videoüberwachung

9.1 Prüfungen zur Videoüberwachung in Fußballstadien abgeschlossen

Meine bereits im Jahr 2016 begonnene umfassende Prüfung der Videoüberwachung in niedersächsischen Fußballstadien konnte im Jahr 2021 abgeschlossen werden. Geprüft wurden Vereine, die in der 1. Bundesliga, der 2. Bundesliga oder der 3. Liga spielen.

Gemäß den „Richtlinien zur Verbesserung der Sicherheit bei Bundesspielen" des Deutschen Fußballbundes müssen in den Stadien der oberen drei Ligen Videoüberwachungsanlagen zum Schutz der Besucherinnen und Besucher installiert werden. Von einer solchen Überwachung können somit alle Personen betroffen sein, die in den höchsten deutschen Fußballigen ein Fußballspiel besuchen.

Es ist mir gelungen, die bereits in meinem 25. Tätigkeitsbericht angekündigten Prüfungen in zwei weiteren Fußballstadien durchzuführen, die bis dato noch ausstanden.

Unangekündigte Kontrolle am Spieltag wirkt

Wie bereits in einem früheren Tätigkeitsbericht ausgeführt, hatte ich an einem Spieltag im Herbst 2019 eine unangekündigte Prüfung der Videoüberwachung in einem Stadion durchgeführt. Die dabei festgestellten unrechtmäßigen Verarbeitungen wurden mittlerweile abgestellt.

Zudem wurde zwischen der Polizei, die ihre Nutzung der Überwachungsanlage auf § 32 Absatz 3 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes stützt, und dem Verein eine Nutzungsvereinbarung geschlossen, die nur noch rechtmäßige Datenverarbeitungen beinhaltet und zulässt.

Abschluss zu zwei weiteren Prüfungen

Im Jahr 2021 konnte ich zudem die zwei noch ausstehenden Prüfungen abschließen. In einem der beiden Stadien fand ich erfreulicherweise keine datenschutzrechtlichen Mängel vor. Zudem hatte ich im Vorfeld eine Datenschutz-Folgenabschätzung erhalten, die alle erforderlichen technisch-organisatorischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten beinhaltete.

Kameras mit unzulässiger Zoom-Funktion

Im anderen Stadion bemängelte ich die Nutzung der Videokameras durch den Verein und seiner Sicherheitskräfte, da mit der Anlage unzulässigerweise herangezoomt, also der Bildausschnitt vergrößert werden konnte. Diese Funktion war nicht erforderlich, um das festgelegte Ziel zu erreichen und wurde unmittelbar abgestellt. Die mit mir getroffenen Absprachen und Änderungen fanden Eingang in eine aktualisierte Nutzungsvereinbarung und eine Datenschutz-Folgenabschätzung, deren Inhalte mir abschließend zu Kenntnis gegeben wurden. Weitere aufsichtsrechtliche Maßnahmen wurden von mir nicht getroffen, da unmittelbar nach meinem Hinweis zu einer datenschutzgerechten Verfahrensweise übergegangen wurde. Zudem wurden die nicht erforderlichen gezoomten Ausschnitte nicht gespeichert, sondern „nur" in Echtzeit betrachtet, so dass keine nachhaltige Verarbeitung durch eine Aufzeichnung stattfand.

Als Gesamtfazit meiner Prüfungen der Videoüberwachungen in den oberen drei Ligen in Niedersachsen konnte ich folgende Hauptmängel identifizieren:

- Es mussten Nutzungsvereinbarungen zwischen den Stadionverantwortlichen und der Polizei ergänzt werden. Wesentliche Vorgehensweisen und technisch-organisatorische Schutzmaßnahmen waren teilweise bei der gemeinsamen Videoüberwachung nicht aufgenommen.
- Videoüberwachungen durch die Sicherheitskräfte des Stadionbetreibers (grundsätzlich bei Veranstaltungen in einem „Echtzeit-Monitoring") waren hinsichtlich der Möglichkeit der Zoomfunktion nicht erforderlich. Es reichten in diesen Fällen Übersichtsaufnahmen.
- Teilweise wurden Aufzeichnungen zu lange gespeichert und aufbewahrt.
- Mängel in der gemeinsamen oder auch getrennten Hinweisbeschilderung. Die Hinweisschilder entsprachen nicht den Transparenzanforderungen der DS-GVO beziehungsweise zeigten nicht die unterschiedlichen Zweckbestimmungen bei gemeinsamer Beschilderung auf.
- Ungeschützt verlegte Kabel für die Übertragung der Videosignale, die im Zweifelsfall durch Besucher sabotiert werden konnten.

Die erkannten Mängel wurden in Teilbereichen unmittelbar und – sofern weitere Maßnahmen erforderlich waren – im Nachgang abgestellt.

Ich behalte mir vor, auch zukünftig einen prüfenden Blick auf Videoüberwachungen in Fußballstadien in Niedersachsen zu haben. Es ergeben sich diesbezüglich regelmäßig Änderungen in den drei höchsten Ligen.

9.2 Anlasslose Prüfung zur Videoüberwachung in Bäckereien

In der Vergangenheit erreichten mich immer wieder Beschwerden zur Videoüberwachung in Bäckereien. Ein häufiger Beschwerdegrund war die Überwachung von Beschäftigten, die in vielen Fällen aufgrund ihrer geringen Einkommen des Diebstahls verdächtigt wurden. Weitere Beschwerden richteten sich gegen die Überwachung von Gästen in den Verzehrbereichen. Aus diesem Grund führte ich 2021 eine anlasslose Prüfung der Videoüberwachung in Bäckereien durch.

Vorrangiges Ziel der Prüfung war es, rechtswidrige Datenverarbeitungen festzustellen und diese anschließend zum Schutz von Beschäftigten und Gäste beseitigen zu lassen. Hierzu wählte ich 20 Unternehmen aus ganz Niedersachsen aus, die zwischen 7 und mehr als 600 Filialen betrieben. In die engere Auswahl einbezogen wurden insgesamt 235 Filialen.

Kein Unternehmen bleibt beanstandungsfrei

Es stellte sich heraus, dass 10 der 20 ausgewählten Unternehmen Videoüberwachungsanlagen in 37 Filialen und Firmensitzen betrieben. Nur bei einem Unternehmen war der Erfassungsbereich so eingerichtet, dass der in sehr geringem Umfang unzulässig erfasste Bereich ganz offensichtlich nicht Ziel der Überwachung war.

Verstöße gegen den Grundsatz der „Rechtmäßigkeit"

Bei sieben Unternehmen wurden Beschäftigtenbereiche wie die Arbeitsbereiche hinter dem Tresen oder Vorbereitungsräume überwacht. Beschäftigte haben jedoch einen Anspruch darauf, bei Ausübung ihrer beruflichen Tätigkeit keiner ständigen Arbeits- und Leistungskontrolle durch den Arbeitgeber oder die Arbeitgeberin zu unterliegen. Lediglich der begründete Verdacht auf eine konkrete Straftat kann nach § 26 Absatz 1 Satz 2 BDSG ein berechtigtes Interesse an der begrenzten Überwachung einzelner Beschäftigter darstellen.
Da diese Voraussetzungen jedoch zumindest nicht dauerhaft zutreffen, sind Bereiche, in denen sich Beschäftigte für einen längeren Zeitraum zur Erledigung ihrer Arbeit aufhalten müssen, während der Arbeitszeiten aus der Erfassung auszunehmen.

Keine ständige Arbeits- und Leistungskontrolle

Bei sechs Unternehmen wurden Sitz- und Verzehrbereiche für Gäste überwacht. Die Schutzbedürftigkeit der Interessen der von der Videoüberwachung betroffenen Personen ist in öffentlich zugänglichen Räumen, in denen sich

Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, besonders hoch einzustufen. Dies trifft auf Sitzbereiche, durch die zu einem längeren Aufenthalt eingeladen werden soll, im besonderen Maße zu. Daher werden die Persönlichkeitsrechte der Betroffenen in diesen Bereichen durch eine ständige Videoüberwachung erheblich beeinträchtigt.

Die Überwachung der Sitzbereiche kann daher aufgrund der Interessenabwägung nicht auf Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden und ist somit während der Geschäftszeiten unzulässig.

Verstöße gegen die Grundsätze der Datenminimierung und Speicherbegrenzung

Bei zwei Unternehmen wurden die aufgezeichneten Bilddaten länger als erforderlich gespeichert. Nach Artikel 17 Absatz 1 Buchstabe a DS-GVO sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zum Erreichen der Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind.

Unverzüglich bedeutet ohne schuldhaftes Verzögern (§ 121 Absatz 1 BGB) und bezieht sich sowohl auf die Prüfung der Aufzeichnungen wie auf deren Löschung. Schuldhaft zögerlich handelt auch, wer Aufzeichnungen länger als notwendig ungeprüft hortet oder Hinweisen auf relevante Vorfälle nicht gleich nachgeht.

Bilder nach 72 Stunden löschen

Unter Berücksichtigung der Grundsätze der Datenminimierung und Speicherbegrenzung nach Artikel 5 Absatz 1 Buchstabe c und Buchstabe e DS-GVO muss eine Aufzeichnung grundsätzlich nach 72 Stunden gelöscht werden.

Ob eine Sicherung des Materials notwendig ist, dürfte unter Berücksichtigung von arbeitsfreien Tagen an den Wochenenden grundsätzlich innerhalb eines Zeitraums von drei Tagen geklärt werden können. Die Notwendigkeit einer längeren Speicherung ist nur ausnahmsweise gegeben, wenn beispielsweise aufgrund von Feiertagen längere Schließzeiten bestehen und die Bilddaten nicht innerhalb von 72 Stunden geprüft werden können.

Verstöße gegen den Grundsatz der Transparenz

Ein Unternehmen hat überhaupt nicht auf die Überwachung hingewiesen, bei sechs Unternehmen wurden die Informationspflichten nicht vollständig erfüllt.

Sofern zulässigerweise Videokameras installiert werden, ist gemäß Artikel 13 DS-GVO durch Hinweisschilder sowohl auf die Videobeobachtung als auch auf die dafür verantwortliche Stelle hinzuweisen. Gegebenenfalls

sind die Kontaktdaten des Datenschutzbeauftragten, die Rechtsgrundlage, der verfolgte Zweck, die Speicherdauer, etwaige Empfänger der Daten und die Betroffenenrechte zu nennen. Die Informationen sollten bei Betreten des überwachten Bereichs erkennbar sein. Eine gestaffelte Information ist möglich; in diesen Fällen muss für Betroffene erkennbar sein, wo sie die fehlenden Informationen finden können – denkbar wäre z. B. ein Verweis auf eine Webseite.

Deutlich auf Videoüberwachung hinweisen

Verstöße gegen formale Verpflichtungen

Zwei Unternehmen führten kein Verzeichnis von Verarbeitungstätigkeiten. Gemäß Artikel 30 Absatz 5 DS-GVO ist ein Verzeichnis von Verarbeitungstätigkeiten auch von Unternehmen, die weniger als 250 Mitarbeiter und Mitarbeiterinnen beschäftigen, zu führen, wenn die Verarbeitung personenbezogener Daten nicht nur gelegentlich erfolgt. In der Regel führt daher jede Videoüberwachung zu der Pflicht, die Verarbeitungstätigkeiten zu beschreiben.

Der häufigste Mangel bei den vorgelegten Beschreibungen der Verarbeitungstätigkeiten war die fehlende oder nur unzureichende Beschreibung der getroffenen technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DS-GVO zum Schutz der personenbezogenen Daten.

Vier Unternehmen haben ihren Datenschutzbeauftragten nicht gemäß Artikel 37 Absatz 7 DS-GVO bei der Aufsichtsbehörde gemeldet.

Getroffene Maßnahmen

Verwarnungen, aber keine Bußgelder

Acht der Unternehmen, deren Videoüberwachung von mir beanstandet wurde, habe ich aufgrund der datenschutzrechtlichen Verstöße gemäß Artikel 58 Absatz 2 Buchstabe b DS-GVO verwarnt. Im Rahmen der anlasslosen Datenschutzprüfung habe ich auf die Einleitung von Bußgeldverfahren verzichtet. Diese habe ich noch nicht als erforderlich angesehen.

Die durchgeführte anlasslose Datenschutzprüfung hat gezeigt, dass eine weitere Sensibilisierung der videoüberwachenden Unternehmen sinnvoll ist. Deshalb wurde der Bäcker-Innungsverband Niedersachsen/Bremen von mir über das Ergebnis der Prüfung unterrichtet und gebeten, diese Informationen an die angeschlossenen Unternehmen weiter zu geben.

Eine Sensibilisierung erschien zudem angebracht, weil mich unabhängig von dieser Prüfung weitere vier Beschwerden zu Videoüberwachungen in Bäckereien erreicht haben.

9.3 Unzulässig überwacht, ungewollt veröffentlicht

Im Internet existieren Webseiten, die Videobilder von ungeschützten Kameras abgreifen und diese öffentlich zugänglich machen. Auf einer solchen Seite waren unter anderem Bilder aus einem Elektronikmarkt in Echtzeit abrufbar. Diese zeigten die Beschäftigten, Kundinnen und Kunden sowie das Grundstück und technischen Anlagen.

Nach einem Hinweis auf die Webseite leitete ich gegenüber dem Unternehmen ein aufsichtsbehördliches Prüfverfahren ein. Aus der Stellungnahme des Unternehmens ging hervor, dass die Überwachung ganztägig mit Bild und Ton durch mehrere Kameras erfolgte. Als Anlass für die Überwachung nannte das Unternehmen den Schutz der Kundinnen und Kunden sowie Beschäftigten, die Wahrung des Hausrechts, die Verfolgung von Straftaten, Vandalismus und anderen Störungen sowie die Geltendmachung zivilrechtlicher Ansprüche. Die Bilddaten wurden in Echtzeit durch den Marktleiter beobachtet und darüber hinaus für eine Woche gespeichert. Eine Datenschutz-Folgenabschätzung lag nicht vor.

Nach Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DS-GVO) ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen der Verantwortlichen oder eines Dritten erforderlich ist. Zudem dürfen nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Audiofunktion muss abgeschaltet werden

Nicht erforderlich zum Erreichen der Zwecke und daher datenschutzwidrig ist die Nutzung der Audiofunktion bei einer Videoüberwachung. Denn das unbefugte Abhören und Aufzeichnen des vertraulich gesprochenen Wortes ist nach § 201 StGB strafbar. Die Audiofunktion war daher zu deaktivieren.

Keine Rechtsgrundlage für Überwachung der Beschäftigten

Auch für die Überwachung der Beschäftigten an den Beratungsplätzen und hinter der Kasse gab es keine Rechtsgrundlage. Beschäftigte haben einen Anspruch darauf, bei Ausübung ihrer beruflichen Tätigkeit keiner ständigen Arbeits- und Leistungskontrolle durch den Arbeitgeber zu unterliegen. Lediglich der begründete Verdacht auf eine konkrete Straftat kann nach § 26 Absatz 1 Satz 2 BDSG ein berechtigtes Interesse an der begrenzten Überwachung einzelner Beschäftigter darstellen.

Bereiche, in denen sich Beschäftigte über einen längeren Zeitraum zur Arbeitserledigung aufhalten sind daher während der Betriebszeiten aus der Erfassung auszunehmen.

Nicht mehr notwendige Videodaten sofort löschen

Die Bilddaten wurden zudem länger gespeichert, als es zum Erreichen der Zwecke erforderlich war. Nach Artikel 17 Absatz 1 Buchstabe a DS-GVO sind die Daten der Videoüberwachung unverzüglich zu löschen, wenn sie zum Erreichen der Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Ob eine Sicherung des Materials notwendig ist, dürfte unter Berücksichtigung von arbeitsfreien Tagen an den Wochenenden grundsätzlich innerhalb eines Zeitraums von 72 Stunden geklärt werden können.

Die Notwendigkeit einer längeren Speicherfrist konnte anhand der vorgetragenen Zwecke nicht begründet werden. Es ist Aufgabe des Verantwortlichen, Strukturen zu schaffen, die ein frühzeitiges Erkennen etwa von Fehlbeständen ermöglichen. Zudem sollte gerade durch die Echtzeitbeobachtung ein Diebstahl frühzeitig erkannt und verhindert werden können.

Weiterhin hätte aufgrund der umfangreichen und systematischen Videoüberwachung öffentlich zugänglicher Bereiche gemäß Artikel 35 Absatz 3 Buchstabe c DS-GVO eine Datenschutz-Folgenabschätzung durchgeführt werden müssen.

Dessen ungeachtet wurde der Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit (Artikel 5 Absatz 1 Buchstabe f DS-GVO) besonders deutlich.

Informationen zu technischen und organisatorischen Maßnahmen: https://t1p.de/technik-organisation

Zwar ist das Ausspähen der verwendeten Kameras durch die Betreiberin oder den Betreiber der Internetseite sowie die Veröffentlichung der Aufnahmen unzulässig. Dieses kann den Inhaber des Elektronikmarktes jedoch nicht entlasten. Die verantwortliche Stelle ist durch die DS-GVO verpflichtet, für die im Rahmen der Videoüberwachung stattfindende Verarbeitung personenbezogener Daten geeignete Sicherungsmaßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dadurch soll der unbefugte Zugriff auf die Kameradaten verhindert werden. Dies ist in einem regelmäßig zu überprüfenden und gegebenenfalls anzupassenden Sicherheitskonzept nachzuweisen (Artikel 5 Absatz 2, Artikel 24 Absatz 1 Satz 2 DS-GVO).

Bußgeldverfahren durchgeführt

Aufgrund der verschiedenen, jeweils zumindest fahrlässig begangenen, Verstöße habe ich ein datenschutzrechtliches Ordnungswidrigkeitenverfahren eingeleitet und eine Geldbuße festgesetzt.

Der Festsetzung der Geldbuße ging eine Erörterung des Verfahrensstandes mit dem verantwortlichen Unternehmen sowie dessen Verteidigung voraus. Ziel der Erörterung war eine Verständigung über die mögliche Bußgeldhöhe (vergleiche dazu Kapitel I.4, S. 90). Die schließlich festgesetzte Geldbuße bewegte sich mit 16.000 Euro am unteren Ende des im Rahmen der Verständigung avisierten Korridors.

Trotz der vorherigen Erörterung wurde gegen den Bußgeldbescheid Einspruch eingelegt. Über diesen wurde im Berichtszeitraum noch nicht abschließend entschieden.

Ausreichende Schutzmaßnahmen erforderlich

Die wenigsten Menschen sind sicherlich damit einverstanden, wenn Bilder aus sensiblen Bereichen, vom eigenen Grundstück oder aus der eigenen Wohnung einem weltweiten Publikum zugänglich gemacht werden. Unabhängig von Verstößen gegen datenschutzrechtliche Vorschriften sollte jede Kamerabetreiberin und jeder Kamerabetreiber darauf achten, dass die Kameras und die Übertragungswege gegen unbefugten Zugriff gesichert werden. Für den gewerblichen Einsatz von Überwachungskameras sind ausreichende und angemessene Sicherungsmaßnahmen jedoch nicht nur bloße Kür, sondern eine Pflicht.