Die Landesbeauftragte für den Datenschutz Niedersachsen

25. Tätigkeitsbericht 2019

Niedersachsen

25. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für das Jahr 2019

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

Verantwortlich: Barbara Thiel

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

Bilder, Grafiken: Seite 33, 41, 54, 111, 155: dpa-infografik,
Seite 80: Land Niedersachsen/LfD Niedersachsen,
Seite 144, 145: LfD Niedersachsen
Bildmotiv Grundlayout: Ingimage,
alle weiteren: ccPhotoCloud

Druck: oeding print GmbH
Erzberg 45, 38126 Braunschweig

Aus Gründen der besseren Lesbarkeit wird in diesem Tätigkeitsbericht grundsätzlich auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Selbstverständlich richtet sich dieser Bericht an die Angehörigen aller Geschlechter.

Inhaltsverzeichnis

A. Vorwort

Das erste volle Kalenderjahr unter Geltung der Datenschutz-Grundverordnung liegt hinter Verarbeitern, Betroffenen und Aufsichtsbehörden. Die öffentliche Aufmerksamkeit – am Anfang getrieben von zum Teil übertriebenen Befürchtungen – hat merklich nachgelassen. Dennoch hat das Thema Datenschutz nicht nur einen kurzfristigen Hype erlebt.

Dank der großen Aufregung rund um die Datenschutz-Grundverordnung (DS-GVO) hat sich bei vielen betroffenen Bürgerinnen und Bürgern[1] ein Bewusstsein um ihre Grundrechte ausgeprägt. Vor allem wissen die Menschen nun, dass sie sich mithilfe der Aufsichtsbehörden gegen Datenmissbrauch wirksam wehren können. Das zeigen eindrucksvoll die mehr als 1800 Beschwerden von Betroffenen, die mein Haus im vergangenen Jahr erreicht haben. Dass daneben auch die Verarbeiter von Daten die neuen Regeln ernst nehmen, verdeutlichen die mehr als 820 Datenschutzverletzungen, die verantwortliche Stellen 2019 gemeldet haben.

Entsprechend stark haben die Aufwände für die Bearbeitung von Beschwerden und Meldungen nach Art. 33 DS-GVO zugenommen. Die Vollzugstätigkeit meines Hauses ist deshalb vor allem reaktiv und weniger von anlasslosen Kontrollen geprägt. Das ist sehr bedauerlich, denn gerade diese unangekündigten Prüfungen erweisen sich immer wieder als sehr effektiv und wirkungsvoll und werden auch auf der europäischen Ebene von uns erwartet.

Aufwände entstehen auch dadurch, dass es inzwischen zahlreiche offene Rechtsfragen zur DS-GVO gibt. In den gut anderthalb Jahren mit der neuen Verordnung ist deutlich geworden, dass es noch ein weiter Weg bis zu einer europaweiten Harmonisierung des Datenschutzrechts ist. Es gibt zwar festgelegte Prozesse, wie die Aufsichtsbehörden in Europa im Streitfall zu einer Einigung kommen sollen. Es gibt mit dem Europäischen Datenschutzausschuss auch ein übergeordnetes Gremium, das entscheidet, wenn die Behörden sich nicht einigen können. Doch dem gegenüber stehen eben zahlreiche Fragen zur DS-GVO, zu denen bisher keine europaweiten Positionierungen vorliegen.

1 Aus Gründen der besseren Lesbarkeit wird in diesem Tätigkeitsbericht grundsätzlich auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Selbstverständlich richtet sich dieser Bericht an die Angehörigen aller Geschlechter.

Barbara Thiel

Diese Fragen werden durch Gerichtsurteile in den nächsten Jahren geklärt werden müssen, was aber dauern kann. Bevor es dazu kommt, ist es vor allem Aufgabe der Aufsichtsbehörden, mit ihrer Vollzugspraxis zur Rechtsgestaltung beizutragen. Wir werden klärungsbedürftige Rechtsfragen identifizieren und auch mit verschärften Sanktionen für Klarheit sorgen müssen.

Doch Kontrolle und Sanktionen können nicht der einzige Weg sein, um dem Datenschutzrecht zu mehr Geltung zu verhelfen. Mindestens genauso wichtig und von der DS-GVO gefordert ist es, Verantwortliche und die Öffentlichkeit aufzuklären, zu informieren und zu sensibilisieren. Meine Behörde bemüht sich nach Kräften, auch diesem Aspekt unserer Arbeit gerecht zu werden, scheitert aber regelmäßig an der mangelnden personellen Ausstattung. Ich danke meinen Mitarbeiterinnen und Mitarbeitern sehr, dass sie sich trotzdem immer wieder aufs Neue mit viel Elan und Engagement den Herausforderungen stellen, die unsere vielfältigen Aufgaben mit sich bringen. Nicht selten formulieren Entscheidungsträger aus Politik und Wirtschaft Erwartungen an mein Haus, Beratung und Aufklärung deutlich auszuweiten. Dies wird nur gelingen, wenn mir der Niedersächsische Landtag die dafür nötigen personellen Ressourcen zugesteht. Die erheblichen Aufstockungen der vergangenen Jahre haben maßgeblich dazu beigetragen, dass meine Behörde jedenfalls einen Teil ihrer Aufgaben in angemessener Weise Rechnung tragen konnte. Nun sollte dieser Weg weiter beschritten werden, um auch den anderen Bereich unseres Aufgabenspektrums gebührend bedienen zu können.

B. Management Summary

Das Wichtigste in Kürze

Internationalisierung und Digitalisierung – diese übergreifenden gesellschaftlichen Themen nehmen auch im Datenschutz allgemein und in der Arbeit meiner Behörde im Speziellen bedeutenden Raum ein. So stellt die europäische Zusammenarbeit der Aufsichtsbehörden mein Haus ebenso vor Herausforderungen wie der zunehmende Einsatz von Künstlicher Intelligenz. Darüber hinaus geben Beschwerden, Pannenmeldungen und anlasslose Kontrollen erste Hinweise darauf, wo es in der praktischen Anwendung des Datenschutzrechts noch Defizite gibt.

Mehr Europa – mehr Aufwand – mehr Klarheit?

1200 Vorgänge aus Europa

Eine große Errungenschaft der Datenschutz-Grundverordnung (DS-GVO) ist die Kooperation der Aufsichtsbehörden auf EU-Ebene, die bei grenzüberschreitenden Datenverarbeitungen festen Regeln folgt. Das Ziel: ein europaweit möglichst einheitlicher Gesetzesvollzug. Für meine Behörde hat dies zu einem enormen Arbeitsaufwand geführt, allein 2019 gingen mehr als 1200 Vorgänge aus dem europäischen Binnenmarktsystem ein.

Erfahrungsbericht aus Deutschland

Es ist deshalb nur folgerichtig, dass die Zusammenarbeit der Aufsicht ein wichtiger Bestandteil der ersten Evaluation zur DS-GVO sein wird. Zu dieser hat auch meine Behörde einen Beitrag geleistet, indem sie am Erfahrungsbericht der deutschen Datenschutzkonferenz (DSK) mitgewirkt hat.

Das Fazit: Das Bewusstsein für einen effektiven Datenschutz in der breiten Öffentlichkeit wurde spürbar gestärkt. Nach wie vor nehmen die Aufsichtsbehörden jedoch von Seiten der Verantwortlichen einen erhöhten Orientierungsbedarf wahr. Das betrifft unter anderem die Informationspflichten und die Reichweite des Rechts auf Auskunft.

Alles digital

Die zunehmende Digitalisierung von Wirtschaft, Wissenschaft und Gesellschaft bietet ganz neue Möglichkeiten, die genutzt und zugleich datenschutzrechtlich eng begleitet werden müssen. Eines der Kernthemen ist dabei der verantwortungsvolle Einsatz von Künstlicher Intelligenz (KI). Mit der Hambacher Erklärung haben sich die Datenschutzaufsichtsbehörden des Bundes und der Länder in diese Diskussion eingebracht und die Berücksichtigung der DS-GVO in KI-Systemen gefordert.

Forderungen zu Künstlicher Intelligenz

KI kommt unter anderem in Sprachassistenten, bei der Krebsprävention oder in automatisierten Fahrzeugen zum Einsatz. Letztere stoßen gerade im Autoland Niedersachsen auf großes Interesse, weshalb meine Behörde sich tatkräftig an einem entsprechenden Arbeitskreis der DSK beteiligt. Das Ziel des Gremiums: Im Gespräch mit dem Verband der Automobilindustrie sollen die Anforderungen der DS-GVO für die Weiterentwicklung des autonomen Fahrens präzisiert werden.

Bedauerlich wenig ereignete sich im Berichtszeitraum dagegen im Schulbereich, konkret in Bezug auf die Niedersächsische Bildungscloud. Meiner Behörde lag bis Ende 2019 immer noch kein prüffähiges Datenschutzkonzept vor, obwohl ich das Kultusministerium mehrfach darauf hingewiesen habe, dass die Cloud auch im Pilotbetrieb datenschutzrechtlichen Anforderungen entsprechen muss.

Auch in weiteren Lebensbereichen hält die Digitalisierung bekanntlich immer stärker Einzug und braucht entsprechende rechtliche Rahmenbedingungen. So war etwa das 2019 verabschiedete Gesetz zur Digitalisierung der niedersächsischen Verwaltung längst überfällig. Es enthält wichtige Regelungen, z. B. zum elektronischen Zugang zur Verwaltung, zu elektronischen Bezahlmöglichkeiten oder zur Einführung der elektronischen Aktenführung. Bedauerlich ist allerdings, dass im Gesetzgebungsverfahren keiner meiner Änderungsvorschläge berücksichtigt wurde und so eine Chance verpasst wurde, die Regelungen zum E-Government möglichst datenschutzfreundlich zu gestalten.

Gesetz zur digitalen Verwaltung überfällig

Durchwachsenes Fazit zur Gesetzgebung

In anderen Fällen berücksichtigte der Gesetzgeber erfreulicherweise die Stellungnahmen meiner Behörde stärker. Positive Beispiele für einen offenen und konstruktiven Austausch sind die Gesetzgebungsverfahren zur Novellierung bzw. Änderung des Niedersächsischen Justizvollzugs-, Verfassungsschutz- und Schulgesetzes.

Weiter Kritik am NPOG

Eher durchwachsen fällt dagegen mein Fazit zum neuen Polizei- und Ordnungsbehördengesetz (NPOG) aus. Zwar konnte der Entwurf im Gesetzgebungsverfahren an vielen Stellen aus Sicht des Datenschutzes verbessert werden. Dennoch blieben zahlreiche Kritikpunkte bestehen, wie etwa der verfassungsrechtlich fragwürdige Einsatz sogenannter Staatstrojaner und die massive Ausweitung der Videoüberwachung im öffentlichen Raum. Es wird in den kommenden Jahren eine wichtige Aufgabe meines Hauses sein zu kontrollieren, wie die Polizei- und Ordnungsbehörden mit ihren Befugnissen umgehen.

Prüfungen in Stadien, Kommunen und Unternehmen

Eine eingehende Prüfung meinerseits steht auch noch für den polizeilichen Messenger NIMes aus. Es ist vollkommen nachvollziehbar, dass die Polizei von den Vorteilen eines Messengers profitieren will. Zugleich ist es auch dringend notwendig, dass dieser die datenschutzrechtlichen Anforderungen erfüllen muss. Sobald mir die Polizei die notwendige Datenschutz-Folgenabschätzung vorlegt, werde ich die technischen Abläufe des Messengers im Detail prüfen.

Die Prüfung zur Videobeobachtung in niedersächsischen Fußballstadien ist dagegen fast abgeschlossen. Abgesehen von einem Fall musste ich hier bisher erfreulicherweise relativ wenige Mängel feststellen. Notwendige Verträge zwischen den Vereinen und der Polizei lagen vor und wurden nach meiner Erkenntnis auch eingehalten. Speicherfristen und die Zugangsregelungen zu den jeweiligen Servern waren ebenfalls nicht zu beanstanden.

Ganz grundsätzlich war das Thema Videobeobachtung einmal mehr ein Schwerpunkt unserer Arbeit. Kameras sind allgegenwärtig, ob am Arbeitsplatz, in Bussen und Bahnen und sogar im Wald. Häufig gehen die Betreiber der Überwachungsanlagen dabei über das Erlaubte hinaus und müssen von meiner Behörde zum gesetzeskonformen Einsatz der Videotechnik ermahnt werden.

Kommunen setzen DS-GVO zu spät um

Ebenfalls Grund zur Kritik ergab sich aus meiner Prüfung zur Umsetzung der DS-GVO in 150 Kommunen. Die meisten der befragten Städte, Landkreise und Gemeinden hatten zum Zeitpunkt der Prüfung die Anforderungen der Verordnung noch nicht erfüllt, obwohl diese bereits ein halbes Jahr gültig war. Der größte Nachholbedarf offenbarte sich bei der Bearbeitung von Datenpannen und der Durchführung von Datenschutz-Folgenabschätzungen (DSFA).

Letzteres hatten die Kommunen mit den 50 Wirtschaftsunternehmen gemeinsam, die ich in einer branchenübergreifenden Prüfung zu ihrem Umgang mit der DS-GVO befragte. Auch sie hatten größtenteils Schwierigkeiten mit der DSFA und darüber hinaus besonders mit dem Bereich des technisch-organisatorischen Datenschutzes. Für Unternehmen, die besonders schlecht abgeschnitten haben, habe ich weitergehende Prüfungen vor Ort angeordnet.

Zweiklang von Vollzug und Aufklärung

Anders als bei den anlasslosen Prüfungen in Kommunen und Unternehmen gehen die meisten Kontrollverfahren meiner Behörde auf die zahlreichen Beschwerden (2019: 1882) und Meldungen von Datenschutzverletzungen (824) zurück. Stelle ich dabei schwerwiegende Verstöße fest, eröffne ich ein Ordnungswidrigkeitenverfahren, in dessen Rahmen auch ein Bußgeld verhängt werden kann. 2018 habe ich noch keine Geldbußen nach DS-GVO ausgesprochen. Im vergangenen Jahr habe ich dagegen aufgrund von 22 Tatvorwürfen Bußgelder in Höhe von fast 480.000 Euro verhängt, die zum großen Teil aber noch keine Rechtskraft erlangt haben. Basis für die Berechnung dieser Sanktionen war das von der DSK entwickelte Bußgeldkonzept. So werden Gerichte nicht nur über die Rechtmäßigkeit des einzelnen Bußgeldes, sondern auch über die Anwendbarkeit dieses Konzepts zu entscheiden haben.

Erste Bußgelder nach DS-GVO verhängt

Aus Defiziten, die ich im Rahmen von Prüfungen feststelle, folgen aber nicht nur aufsichtsbehördliche Maßnahmen. Ich nehme sie auch zum Anlass, das Informations- und Sensibilisierungsangebot meiner Behörde zu erweitern. Denn die DS-GVO soll nicht nur zu einer verschärften Durchsetzung des Datenschutzrechts führen. Zugleich gibt sie uns Aufsichtsbehörden auch auf, Verantwortliche, Betroffene und die Öffentlichkeit im Allgemeinen zu informieren und zu sensibilisieren. Deshalb habe ich auch 2019 wieder zahlreiche Informationsmaterialien veröffentlicht und viele Vorträge vor sehr unterschiedlichen Zielgruppen gehalten. Erstmals beteiligt haben sich zudem meine Mitarbeiterinnen und Mitarbeiter an der Initiative „Datenschutz geht zur Schule", die Kinder und Jugendliche für den sicheren Umgang mit digitalen Medien sensibilisieren will. Die Rückmeldungen dazu fielen so positiv aus, dass sich meine Behörde nun jährlich an dieser Aktion beteiligen wird, um möglichst viele Schülerinnen und Schüler in Niedersachsen zu erreichen.

„Datenschutz geht zur Schule"

Informationen zu Fotos und Technik

Eine Frage, die im Übrigen in den Schulvorträgen behandelt wird, ist, was bei der Veröffentlichung von Fotos beachtet werden muss. Dieses Problem treibt nicht nur Jugendliche um, sondern auch Verantwortliche in Vereinen, öffentlichen Stellen und Unternehmen. Deshalb widmet sich ein ganzes Unterkapitel des Tätigkeitsberichts diesem Thema und beleuchtet es von verschiedenen Seiten.

Mehr Raum als in vergangenen Jahren nehmen außerdem technisch geprägte Themen ein. Dies liegt zum einen an den Aktivitäten zum Standard-Datenschutzmodell (SDM) und zum Prozess zur Auswahl angemessener technisch-organisatorischer Sicherungsmaßnahmen (ZAWAS). Letzteres wird nun auch verstärkt in der Praxis angewendet. Zum anderen ist die notwendige Auseinandersetzung mit der Bedrohung durch den Trojaner Emotet eine Ursache für diesen Schwerpunkt. Und zum dritten thematisiere ich die Bemühungen meiner Behörde um eine Haltung zur Nutzung von Windows 10. Ein Arbeitskreis der DSK hat sich unter meiner Leitung mit der Frage beschäftigt, wie Windows 10 datenschutzrechtlich bewertet werden kann. Als erstes Ergebnis wurde ein Prüfschema veröffentlicht, anhand dessen Verantwortliche beurteilen können, ob der Einsatz von Windows 10 in ihrer Organisation datenschutzkonform ist oder wäre.

Prüfschema zu Windows 10

C. Europäischer Datenschutz

C.1. Neues vom EDSA – Mehr Klarheit für Europa

Mit Geltungsbeginn der Datenschutz-Grundverordnung nahm der neu gegründete Europäische Datenschutzausschuss seine Arbeit auf. Der Ausschuss soll eine einheitliche Anwendung der DS-GVO sicherstellen und veröffentlichte zu diesem Zweck auch im Jahr 2019 Leitlinien und Stellungnahmen.

In seinem Arbeitsplan für das Jahr 2019 hatte sich der Europäische Datenschutzausschuss (EDSA) unterschiedliche Themen vorgenommen, die der Auslegung in Leitlinien und Stellungnahmen bedurften. Dazu zählten z. B. der internationale Datenverkehr, die Betroffenenrechte oder die Zusammenarbeit der Aufsichtsbehörden.

Zudem galt es, zu aktuellen Entwicklungen im Datenschutzrecht Stellung zu nehmen sowie Anfragen von verschiedenen Stellen aus Politik und Verwaltung zu beantworten. Auch der eine oder andere Dissens unter den Aufsichtsbehörden zur Auslegung der DS-GVO oder zu Verfahrensfragen war zu klären.

Leitlinien zu Videoüberwachung und Verhaltensregeln

Die DS-GVO als neues Recht brachte zunächst viele offene Fragen und ein unterschiedliches Verständnis einzelner Regeln mit sich. Auch nach mehr als einem Jahr Geltungsdauer besteht nach wie vor Bedarf an Erläuterung und gemeinsamer Auslegung der verschiedenen Regelungen. Der EDSA veröffentlichte daher auch im Jahr 2019 wesentliche Auslegungshilfen in Form von Leitlinien zur Anwendung der DS-GVO. Diese Leitlinien bilden ein breites Spektrum verschiedener Themen und Einzelfragen des Datenschutzrechts ab. Die neuen Leitlinien zu Verhaltensregeln nach Art. 40 und 41 DS-GVO befassen sich etwa mit der Möglichkeit, die Einhaltung der Verordnung mit Hilfe von Verhaltensregeln („Code of Conduct") nachweisen zu können. Bestimmte wirtschaftliche Sektoren können nach diesen Regeln auf sie zugeschnittene, praktische Datenschutzvorschriften vereinbaren. Die Leitlinien unterstützen

Guidelines des EDSA:
https://t1p.de/Guidelines

bei der Erstellung solcher Verhaltensregeln. Außerdem regeln sie, wie die Einhaltung der Verhaltensregeln überwacht werden soll.

Zu ganz speziellen Fragenstellungen hat der EDSA in seinen zweiten Leitlinien im Jahr 2019 Auslegungshilfe gegeben: Die Rechtsgrundlage des Art. 6 Abs. 1 lit. b DS-GVO im Zusammenhang mit Online-Services. Nach Art. 6 Abs. 1 lit. b DS-GVO ist eine Datenverarbeitung erlaubt, wenn sie zur Erfüllung eines Vertrages erforderlich ist. Gerade im Bereich des Internets stellen sich hierzu Einzelfragen, die der EDSA in den Leitlinien aufgreift, z. B. wie bei der Bündelung mehrerer separater Online-Services vorgegangen wird und welche datenschutzrechtlichen Folgen die Aufhebung des Vertrages hat (siehe hierzu auch Kapitel C. 4, S. 24)

Ein weiteres Thema, mit dem sich der EDSA auseinandergesetzt hat, ist die Verarbeitung personenbezogener Daten durch Videoüberwachung. Die Leitlinien enthalten Klarstellungen zu möglichen Rechtsgrundlagen für eine Videoüberwachung, zur Weitergabe von aufgezeichneten Daten an Dritte, zu den Betroffenenrechten und zu technisch-organisatorischen Maßnahmen.

Auch zu technischen Themen äußerte sich der EDSA in Leitlinien: Die Grundsätze des Data Protection by Design und by Default wurden erläutert und mit Beispielen unterlegt. Für viele Anwender sind diese Leitlinien eine willkommene Hilfestellung zur Frage, wie technisch-organisatorische Maßnahmen dem Gebot einer datenschutzfreundlichen (Vor-)Einstellung gerecht werden können.

Weiter verabschiedete der EDSA eine aktualisierte Version der Leitlinien zum örtlichen Anwendungsbereich der DS-GVO. Diese wurden nach einer öffentlichen Konsultation überarbeitet. Die Leitlinien legen das Marktortprinzip und die in Art. 3 DS-GVO niedergelegten Kriterien zur Anwendung der DS-GVO auf Datenverarbeiter in den verschiedenen Ländern dar. Dies ist besonders wesentlich für Datenverarbeiter außerhalb der EU, die sich im europäischen Markt bewegen und daher unter den Anwendungsbereich der DS-GVO fallen. Die Leitlinien erläutern die verschiedenen möglichen Fallgestaltungen in diesem Zusammenhang.

Zuletzt nahm der EDSA Leitlinien zum Recht auf Vergessenwerden bei Suchmaschinen an. Diese geben Auslegungshinweise zum Recht auf Löschung

nach Art. 17 DS-GVO im Zusammenhang mit dem „Delisting" bei Suchmaschinen, also dem Entfernen einer Seite aus dem Suchindex. Die Leitlinien befanden sich Ende 2019 in der öffentlichen Konsultation.

Stellungnahmen zu Wahlen und Cloud Act

Nachdem bekannt geworden war, dass politische Parteien und Vereinigungen ausgefeilte Profiling-Verfahren zur Überwachung und Adressierung von Wählern nutzen (Stichwort: Cambridge Analytica), veröffentlichte der EDSA eine Stellungnahme zur Verwendung personenbezogener Daten im Rahmen politischer Kampagnen. Diese Stellungnahme zählt wesentliche Punkte auf, die bei der Verarbeitung personenbezogener Daten durch politische Parteien im Zusammenhang mit Wahlen zu beachten sind: Politische Meinungen sind als besondere Kategorie von Daten durch die DS-GVO besonders geschützt. Auch von den Wählern selbst öffentlich gemachte Informationen mit Personenbezug (z. B. in sozialen Netzwerken) unterliegen nach wie vor dem Datenschutzrecht. Profiling ist nur in den engen Grenzen der DS-GVO erlaubt, Transparenz und Informationspflichten sind zu beachten. Die Einhaltung der Datenschutzregelungen ist wesentlich, um das Vertrauen der Wähler in die Integrität der Wahlen zu erhalten.

Politische Meinungen besonders geschützt

Weiter äußerte sich der EDSA ausführlich in einem Brief an den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) des EU-Parlaments zu den Auswirkungen des US-CLOUD Acts auf die europäischen Datenschutzregelungen. Hier geht es um die Pflicht zur Übermittlung von Daten an US-Behörden auf Anfrage, auch wenn die betroffenen Unternehmen die Daten innerhalb der EU verarbeiten. Nach der DS-GVO ist eine solche Herausgabe nur unter sehr engen Voraussetzungen zulässig (siehe D.1, S. 26).

Zusammenarbeit und Zuständigkeiten der Aufsicht

Neben Auslegungshilfen für Datenverarbeiter und Betroffene beschäftigte sich der EDSA auch mit der internen Zusammenarbeit der Aufsichtsbehörden und mit Zuständigkeitsfragen.

Eine wichtige Stellungnahme stellt z. B. klar, welche Aufsichtsbehörde zuständig ist, wenn sich die Niederlassung einer datenverarbeitenden Stelle in der EU verändert oder eine Niederlassung innerhalb der EU aufgegeben wird. Die Zuständigkeit ist dabei besonders unter dem Gesichtspunkt der Zusammenarbeit der Aufsichtsbehörden in grenzüberschreitenden Fällen zu klären. Im Ergebnis kann sich die Zuständigkeit einer Aufsichtsbehörde ändern, jedenfalls solange keine endgültige Entscheidung getroffen wurde.

Klärung von übergeordneten Rechtsfragen

Außerdem befasste sich der EDSA 2019 mit dem Umgang mit Art. 64 Abs. 2 DS-GVO. Nach dieser Regelung können allgemeine Rechtsfragen von genereller Bedeutung für alle Mitgliedstaaten auf Antrag einer einzelnen Aufsichtsbehörde vom EDSA geprüft werden. Der EDSA definiert in seiner Stellungnahme, wann es sich um eine allgemeine Frage handelt, insbesondere in Abgrenzung zu konkreten Verfahren. Dies war zwischen den Aufsichtsbehörden durchaus umstritten. Insbesondere soll durch die Stellungnahme des EDSA verhindert werden, dass die detaillierten Verfahrensregelungen bei der Bearbeitung von Einzelfällen durch einen Antrag auf Klärung allgemeiner Fragen umgangen werden.

Mit einem weiteren internen Dokument verdeutlichte der EDSA die Kriterien für einen so genannten nur lokalen Fall. Bei diesem handelt es sich um einen zwar grenzüberschreitenden Fall, welcher aber lediglich Auswirkungen in einem Mitgliedstaat hat. Hier wurden Kriterien zur Festlegung der Zuständigkeit und zur Behandlung von Beschwerden in diesem Zusammenhang festgelegt. Fragen rund um die Rechtsfigur des nur lokalen Falls hatten immer wieder zu Missverständnissen geführt.

Ausblick

Die Expert Subgroups des EDSA arbeiten weiter an wichtigen Themen. Beispielsweise ist für 2020 die Veröffentlichung von Leitlinien zu Art. 46 und 48 DS-GVO (internationaler Datenverkehr) vorgesehen. Die Auslegung der Betroffenenrechte steht ebenfalls im Fokus. Auch sollen schon bestehende Leitlinien mit Blick auf die DS-GVO überarbeitet werden, so z. B. zum Begriff des Verantwortlichen und des Auftragsverarbeiters.

Die Tätigkeiten des EDSA sind für die Aufsichtsbehörden von besonderer Bedeutung. Durch Leitlinien und Stellungnahmen werden wichtige Auslegungshilfen gegeben, an welche sich die Aufsichtsbehörden gebunden fühlen. Ich werde daher weiterhin die Tätigkeit des Ausschusses aktiv unterstützen.

C.2. Europäische Zusammenarbeit der Aufsichtsbehörden

Eine wesentliche Errungenschaft der Datenschutz-Grundverordnung ist die Zusammenarbeit der Aufsichtsbehörden auf EU-Ebene. Bei grenzüberschreitenden Datenverarbeitungen sind die Datenschutzaufsichtsbehörden verpflichtet, in einem strukturierten Verfahren zusammenzuarbeiten und aufsichtsrechtliche Entscheidungen untereinander abzustimmen. Dies dient dem Ziel, einen europaweit einheitlichen Gesetzesvollzug zu gewährleisten.

Seit Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) prüft meine Behörde alle eingehenden Beschwerden und sonstigen Eingaben zunächst darauf, ob eine grenzüberschreitende Verarbeitung im Sinne von Art. 4 Nr. 23 DS-GVO vorliegt. Ist das der Fall, wird das europäischen Kooperationsverfahren nach Art. 60 ff. DS-GVO angewendet. Es greift das Prinzip des One-Stop-Shop, wobei eine federführende Aufsichtsbehörde bestimmt wird, welche mehrere andere betroffene Aufsichtsbehörden im festgelegten Kooperationsverfahren beteiligt. Federführende Aufsichtsbehörde ist nach Art. 56 Abs. 1 DS-GVO die Behörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen in der EU. Diese ist dann Ansprechpartnerin für den Verantwortlichen oder Auftragsverarbeiter.

Prinzip des One-Stop-Shop

Identifizierung der federführenden Behörde

Bei einer grenzüberschreitenden Verarbeitung ist meine Behörde somit zunächst verpflichtet, ein Verfahren nach Art. 56 Abs. 1 DS-GVO zur Identifizierung der federführenden Aufsichtsbehörde einzuleiten. Sie übermittelt zu diesem Zweck den Vorgang den anderen europäischen Aufsichtsbehörden über das Internal Market Information (IMI) System. Diese Vorgehensweise findet lediglich dann keine Anwendung, wenn die federführende Aufsichtsbehörde in einem früheren Verfahren nach Art. 56 DS-GVO für eine bestimmte Verarbeitung durch einen bestimmten Verantwortlichen bereits identifiziert worden ist. 2019 hat meine Behörde 27 Verfahren zur Identifizierung der federführenden Aufsichtsbehörde im IMI-System eingeleitet.

Daneben erhält meine Behörde regelmäßig eine Vielzahl von Benachrichtigungen im IMI-System, dass eine andere europäische Aufsichtsbehörde ein Verfahren nach Art. 56 DS-GVO zur Identifizierung der federführenden Aufsichtsbehörde eingeleitet hat. In jedem dieser Fälle ist zu prüfen, ob meine Behörde betroffene oder federführende Aufsichtsbehörde ist. 2019 hat meine Behörde mehr als 850 Vorgänge zur Identifizierung der federführenden Aufsichtsbehörde über das IMI-System erhalten. In mehr als 320 Fällen haben wir entschieden, als betroffene Aufsichtsbehörde am Verfahren teilzunehmen. In drei Fällen sind wir federführend.

320 mal betroffen, 3 mal federführend

Erst nachdem die federführende Aufsichtsbehörde identifiziert worden ist, beginnt das eigentliche Abstimmungsverfahren aufsichtsrechtlicher Entscheidungen unter den betroffenen Behörden nach Art. 60 DS-GVO. Können sich die Aufsichtsbehörden nicht einigen, wird das Kohärenzverfahren nach Art. 63 ff. DS-GVO eingeleitet, in dem letztlich der Europäische Datenschutzausschuss eine verbindliche Entscheidung trifft.

Darüber hinaus sieht die DS-GVO ein Verfahren für die gegenseitige Amtshilfe (Art. 61 DS-GVO) sowie für gemeinsame Maßnahmen der Aufsichtsbehörden vor, bei welchem insbesondere gemeinsame Untersuchungen und Durchsetzungsmaßnahmen möglich sind (Art. 62 DS-GVO).

Erstes Fazit: Stark gestiegener Aufwand

Das vergangene Jahr hat gezeigt, dass die Zusammenarbeit über das IMI-System einen enormen Anstieg an Vorgängen zur Folge hatte, die zu koordinieren und zu bearbeiten waren. Allein im Berichtszeitraum sind in meiner Behörde insgesamt mehr als 1200 Vorgänge aus dem europäischen Raum eingegangen. Hierzu zählen neben den Verfahren zur Identifizierung der federführenden Behörde auch Abstimmungen zu Kooperations- oder Kohärenzverfahren sowie informelle Abstimmungen zwischen den Aufsichtsbehörden. Auch in Fällen, in denen meine Behörde letzten Endes nicht beteiligt war, mussten meine Mitarbeiterinnen und Mitarbeiter zunächst prüfen, ob eine Teilnahme am Verfahren erforderlich ist.

Um sicherzustellen, dass die Aufsichtsbehörden über jedes neu eingeleitete Verfahren mit europäischem Bezug sowie über sämtliche weitere Verfahrensschritte der anderen Aufsichtsbehörden informiert werden, sendet das IMI-System Benachrichtigungen. Die Vielzahl dieser Benachrichtigungen hat neben der großen Anzahl der zu bearbeitenden Fälle zu einem sehr hohen Informationsaufkommen und einem hohen Arbeitsaufwand für meine Behörde geführt.

Zentrale Stelle zur Koordinierung

Bewältigt wurden die Verfahren mit europäischem Bezug mithilfe der neu in meiner Behörde eingerichteten zentralen Kontaktstelle zur Koordinierung der europäischen Kooperationsverfahren. Dieses Vorgehen hat sich sehr bewährt. Die Konzentrierung der Verfahren hat dazu geführt, dass diese im IMI-System einheitlich und fristgerecht abgearbeitet werden konnten und eine Beteiligung an allen uns betreffenden Verfahren gewährleistet werden konnte.

Das europäische Kooperationsverfahren ist zwar zeitaufwendig und komplex und bindet zudem verhältnismäßig hohe Personalkapazitäten. Doch es hat sich gezeigt, dass durch die Anwendung des One-Stop-Shop bislang ganz überwiegend zufriedenstellende Ergebnisse erzielt werden konnten.

Gleichzeitig wurde im vergangenen Jahr jedoch mitunter sichtbar, dass das Konzept des One-Stop-Shop dazu führen kann, dass bestimmte Aufsichtsbehörden – abhängig von der Anzahl niedergelassener Datenverarbeiter in ihrem Zuständigkeitsbereich – mit einer deutlich höheren Zahl von grenzüberschreitenden Fällen konfrontiert sind als andere. Fraglich ist, ob und inwieweit sich dieser Umstand zukünftig auf die Dauer der Verfahren und somit auf die wirksame Durchsetzung der DS-GVO sowie deren Akzeptanz auswirken wird. Es kann mit Spannung auf den für Mai 2020 vorgesehenen ersten Kommissionsbericht zur Evaluierung der DS-GVO geblickt werden, der ebenfalls ein erstes Fazit zur europäischen Zusammenarbeit der Aufsichtsbehörden enthalten wird.

C.3. Evaluation der DS-GVO

Der europäische Gesetzgeber verfolgte mit der umfassenden Neuregelung des Datenschutzes verschiedene Ziele wie vor allem die Harmonisierung des Datenschutzrechts sowie des Vollzugs innerhalb der EU. Um zu prüfen, wie wirksam die neuen Regelungen in der Praxis sind, wird die Datenschutz-Grundverordnung evaluiert. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) beteiligt sich daran unter anderem mit einem eigenen Evaluationsbericht.

Art. 97 der Datenschutz-Grundverordnung (DS-GVO) verpflichtet die EU-Kommission zur Vorlage eines Berichtes über die Bewertung und Überprüfung der Verordnung an das EU-Parlament und den Rat. Erstmals muss dies bis zum 25. Mai 2020 geschehen und anschließend in einem Vier-Jahres-Rhythmus. Die Evaluation soll die Basis für Entscheidungen über Änderungen oder Weiterentwicklungen des bestehenden Rechtsrahmens bilden. Besonders im Fokus: die Anwendung und Wirkungsweise der Vorschriften zum internationalen Datenverkehr und zur Zusammenarbeit der Aufsichtsbehörden in Europa. Die EU-Mitgliedstaaten und die einzelnen Aufsichtsbehörden sind aufgerufen, Informationen aus ihren eigenen Erfahrungen in der praktischen Anwendung der DS-GVO beizusteuern. Nach dem Gesetzeswortlaut sollen bei Änderungen der Verordnung insbesondere Entwicklungen in der Informationstechnologie und Fortschritte in der Informationsgesellschaft berücksichtigt werden.

Funktioniert die DS-GVO?

Im Fokus: Internationaler Datenverkehr und Kooperation der Behörden

Mit der Evaluation der DS-GVO sollen vor allem praktische Umsetzungsprobleme erkannt und verdeutlicht werden. Dabei hat der Gesetzgeber insbesondere die Regelungen zur grenzüberschreitenden Zusammenarbeit der Aufsichtsbehörden bewertet, da diese neu eingeführt wurden und zu neuen Verfahrensabläufen führten. Hier ist die Frage zu betrachten, ob diese neuen Verfahren angemessen funktionieren.

Durch den Verweis auf den technologischen Fortschritt und neue Technologien sollen auch mögliche zukünftige Regelungsbereiche frühzeitig identifiziert und bereits jetzt in die Bewertung mit einbezogen werden. Ergeben sich etwa neue Gefahren für Persönlichkeitsrechte Betroffener durch technologische Entwicklungen, ist zu prüfen, ob die DS-GVO diesen Rechnung tragen kann oder kurz- bzw. längerfristig rechtliche Anpassungen und Weiterentwicklungen nötig sind.

Letztlich beeinflussen die Evaluation und die zugrunde liegenden Berichte aus den Mitgliedstaaten wesentlich die weitere Entwicklung des Datenschutzrechts und führen im besten Fall zu dessen Optimierung.

Die Kommission begann den Evaluationsprozess im November 2019 mit der Versendung eines Fragebogens an die europäischen Datenschutzaufsichtsbe-

hörden. Entsprechend den Vorgaben des Art. 97 Abs. 2 DS-GVO enthielt dieser vor allem Fragen zu Angemessenheitsentscheidungen der Kommission zur Datenübermittlung in Drittstaaten sowie zur Anwendung und Wirkungsweise der europäischen Kooperations- und Kohärenzverfahren. Daneben wurden Zahlen zur Ausstattung der Aufsichtsbehörden sowie zu Beschwerden und Meldungen von Datenschutzverletzungen abgefragt. Mitte Dezember 2019 wurde von Deutschland eine unter den Aufsichtsbehörden abgestimmte Antwort verschickt.

Zusätzlicher Input aus Deutschland

Die deutschen Aufsichtsbehörden haben daneben die Möglichkeit wahrgenommen, weitere eigene Beiträge zur Evaluierung der DS-GVO zu liefern. Im November 2019 wurde ein Erfahrungsbericht der DSK beschlossen und anschließend an den Europäischen Datenschutzausschuss (EDSA) versandt, der die Beiträge der europäischen Aufsichtsbehörden sammelt.

Erfahrungsbericht zum Download: https://t1p.de/DSK-Erfahrung

Den in der DSK zusammengeschlossenen deutschen Aufsichtsbehörden war es ein Anliegen, eigene Erfahrungen in der Anwendung der DS-GVO zusammenzustellen und in den Optimierungsprozess einzubringen. Dabei ziehen die Behörden insgesamt eine positive Bilanz. Das Bewusstsein für einen effektiven Datenschutz in der breiten Öffentlichkeit wurde spürbar gestärkt. Die Zahl der Beratungsanfragen und Beschwerden stieg deutlich an. Die neuen Regeln werden nach Erfahrung der DSK in der Praxis zunehmend angenommen, auch wird Datenschutz in der Wirtschaft vermehrt als Wettbewerbsvorteil gesehen.

Positiv zu bewerten sind besonders die gestärkten Befugnisse der Aufsicht zur Durchsetzung des Datenschutzrechts (wozu auch der deutlich erhöhte Bußgeldrahmen gehört) und die engere Zusammenarbeit der Aufsichtsbehörden im europäischen Raum. Beides ermöglicht eine effektivere Durchsetzung der Datenschutzregelungen. Nach wie vor nehmen die Aufsichtsbehörden jedoch einen erhöhten Bedarf an Orientierung für die datenverarbeitenden Stellen wahr.

Erfahrungen aus der praktischen Anwendung

Der Evaluationsbericht der DSK schildert Erfahrungen aus der praktischen Anwendung der neuen Regelungen, nennt Änderungsbedarf und zeigt Probleme auf. Der Bericht konzentriert sich auf identifizierte Schwerpunktthemen, welche in besonderem Maße bei den deutschen Aufsichtsbehörden aufgefallen sind.

Probleme mit den Informationspflichten

Dazu gehört die Umsetzung der Informationspflichten in einem analogen Umfeld und in bestimmten, häufig vorkommenden Alltagssituationen. Beispielsweise macht die umfassende Erfüllung der Informationspflichten bei einem telefonischen Erstkontakt, etwa zur Terminvereinbarung, oder bei einem Vertragsabschluss per Telefon Probleme. Hier geht es um praktikablere und auch bürgerfreundlichere Lösungen für eine angemessene datenschutzrechtliche Transparenz.

Ein weiteres Schwerpunktthema bildet die Regelung zur Meldung von Datenschutzverletzungen. Die Aufsichtsbehörden verzeichnen eine hohe Zahl dieser Meldungen, obwohl bei näherer Betrachtung die Voraussetzungen dafür in vielen Fällen gar nicht vorliegen. Hier besteht offenkundig eine große Unsicherheit bei den datenverarbeitenden Stellen; eine Klarstellung im Gesetz erscheint notwendig. Die DSK spricht sich hier dafür aus, die Meldepflicht nach Art. 33 DS-GVO auf Fälle zu beschränken, die voraussichtlich zu einem mehr als nur geringen Risiko für die Rechte und Freiheiten natürlicher Personen führen.

In der alltäglichen Anwendung stellen sich zudem verschiedene Fragen zur Zusammenarbeit der Aufsichtsbehörden im europäischen Raum und im Kohärenzverfahren vor dem EDSA. Dies ist dem Umstand geschuldet, dass es sich hier um völlig neue Verfahren und Formen der verwaltungsrechtlichen Zusammenarbeit handelt. Nach den Erfahrungen in der Praxis ist festzustellen, dass zum Teil eine unterschiedliche Auslegung der Vorschriften oder Unklarheiten im Gesetzestext zu Verzögerungen bzw. Unstimmigkeiten im Verfahren führen können.

Umsetzung von Privacy by Design

Auch das neue Prinzip des Privacy by Design wird zwar als zu begrüßende Neuerung angesehen, welche den Datenschutz insgesamt aufwertet. In der Praxis ist die Umsetzung allerdings fraglich, da ausgerechnet die Hersteller von Hard- und Software von der DS-GVO nicht unmittelbar in die Pflicht genommen werden. Ein weiterer Schwerpunkt des Berichts sind Fragen rund um den Grundsatz der Zweckbindung, z. B. im Zusammenhang mit der Erlaubnis zur Weiterverarbeitung von Daten.

Erfahrungen aus Niedersachsen

Ich begrüße und unterstütze den unter Mitarbeit von Niedersachsen erstellten Bericht der DSK. Zu einem Großteil betreffen die dort abgebildeten Probleme und Fragen auch meine Behörde in ihrer Beratungs- und Aufsichtstätigkeit.

Die meisten der von Niedersachsen aufgeworfenen Fragen und Problemfelder finden sich im finalen Evaluationsbericht der DSK wieder. Aus meiner Sicht ist etwa die Alltagstauglichkeit der Informationspflichten immer wieder ein schwieriges Thema. Die Pflichten sind in einer digitalen Umgebung verhältnismäßig einfach zu erfüllen, bei den immer noch zahlreichen nicht-digitalen Verfahren der Datenerhebung ist das mitunter deutlich schwieriger und bürokratischer. Ich freue

mich, dass wir im Rahmen unserer Mitarbeit am Evaluationsbericht die Möglichkeit hatten, dem Gesetzgeber unsere Erfahrungen zu diesem Thema zur Kenntnis zu geben.

Wie weit reicht das Recht auf Auskunft?

Ein weiterer, auch aus niedersächsischer Sicht wichtiger Punkt bei der Bewertung der DS-GVO ist das Recht auf Auskunft und damit einhergehend das Recht auf Kopie. In der Beratungs- und Vollzugspraxis hat die Umsetzung dieser Rechte zu vielen Fragen geführt, für welche die DS-GVO keine Lösungsmöglichkeiten anbietet. Dies betrifft vor allem Fälle, in welchen sehr große Datenmengen im Fokus stehen. Ich wünsche mir eine Klarstellung des Gesetzgebers zur Reichweite und zum Umfang des Rechts auf Auskunft.

Des Weiteren berücksichtigt der Evaluationsbericht der DSK wichtige, auch von Niedersachsen aufgeworfene Probleme im Zusammenhang mit den neuen europäischen Kooperationsverfahren. Die gesetzlich festgelegten, sehr kurzen Verfahrensfristen sind für alle Beteiligten schwierig einzuhalten und können dazu führen, dass die angemessene Behandlung eines Falles nur eingeschränkt möglich ist. Daneben besteht eine Regelungslücke im Kohärenzverfahren für den Fall, dass ein Beschlussentwurf aufgrund einer Stellungnahme des EDSA geändert wurde. Da eine weitere Rückmeldung des Ausschusses, dass seinen Bedenken Rechnung getragen wurden, nicht vorgesehen ist, kann sich in der Praxis die Frage stellen, ob und inwieweit ein geänderter Beschlussentwurf sogleich rechtsverbindlich wird.

C.4. Datenverarbeitung zur Vertragserfüllung – Leitlinien des EDSA

Was Gegenstand eines Vertrags ist, obliegt grundsätzlich der Entscheidung der Vertragsparteien. Dies bedeutet jedoch nicht, dass Datenverarbeitungen allein deshalb gemäß Art. 6 Abs. 1 lit. b DS-GVO erlaubt sind, weil sie im Vertragstext genannt werden.

Art. 6 Abs. 1 lit. b DS-GVO erlaubt Datenverarbeitungen, die der Erfüllung oder dem Abschluss eines Vertrags dienen. Doch welche Verarbeitungen personenbezogener Daten können auf diese Norm gestützt werden? Der Europäische Datenschutzausschuss (EDSA) hat in den Leitlinien 2/2019 „on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects" (Version 2.0) eine umfassende Bewertung zu dieser Frage im Zusammenhang mit Online-Dienstleistungen vorgenommen.

Guidelines des EDSA: https://t1p.de/Guidelines

Voraussetzungen: Wirksamer Vertrag und Erforderlichkeit

Wer eine Ware bei einem Versandhändler bestellt, gibt seine Anschrift zum Versand und seine Zahlungsdaten preis, um den offenen Betrag zu begleichen. Der Händler kann sich bei der Nutzung dieser Daten zur Abwicklung des Kaufs auf die Rechtsgrundlage des Art. 6 Abs. 1 lit. b DS-GVO berufen.

Damit Unternehmen und Behörden Datenverarbeitungen zur Vertragserfüllung auf Art. 6 Abs. 1 lit. b DS-GVO stützen können, müssen zwei Voraussetzungen erfüllt sein. Der Vertrag muss nach nationalem Recht wirksam zustande gekommen und die Datenverarbeitung muss objektiv zur Vertragserfüllung erforderlich sein. Es ist also nicht ausreichend, wenn die Datenverarbeitung zur Vertragserfüllung lediglich nützlich ist. Darüber hinaus reicht es nicht aus, dass die Datenverarbeitung von den Allgemeinen Geschäftsbedingungen (AGB) eines Website-Betreibers gedeckt ist.

AGB auf Website reichen nicht aus

Die Datenverarbeitung muss mit der vertragstypischen Leistung so eng verknüpft sein, dass die Leistung ohne sie nicht erbracht werden kann. Die Beurteilung dessen, was vertragstypisch ist, hängt von den wesentlichen Merkmalen des jeweiligen Vertrags und den Erwartungen der Vertragsparteien ab. Bei Verträgen, die verschiedene unterschiedliche Vertragstypen vereinen (sog. typengemischter Vertrag), muss jede vertragstypische Leistung isoliert betrachtet werden. Dient die Datenverarbeitung der Umsetzung eines nicht vertragstypischen Inhalts, müssen die Voraussetzungen einer anderen Rechtsgrundlage des Art. 6 Abs. 1 DS-GVO erfüllt sein.

Erfasste und nicht erfasste Fälle

Art. 6 Abs. 1 lit. b DS-GVO legitimiert nicht nur die Datenverarbeitungen, die mit dem Austausch der vertraglichen Leistungen einhergehen. Die Rechtsgrundlage greift auch für Datenverarbeitungen, die im Fall unterbliebener oder verspäteter Leistungen (z. B. Mahnung wegen unterlassener Zahlung, Produktreklamationen), im Widerrufs-, Rücktritts- oder Kündigungsfall erfolgen. Auch die weitere Aufbewahrung von Daten für den Garantie- oder Gewährleistungsfall lässt sich noch auf diese Rechtsgrundlage stützen.

Art. 6 Abs. 1 lit. b DS-GVO ist dagegen keine geeignete Rechtsgrundlage, wenn die Datenverarbeitung der Optimierung der Website, der Betrugsprävention oder personalisierten Werbeanzeigen dient.

Keine personalisierte Werbung

Werden die Daten allerdings zur Personalisierung von Inhalten verarbeitet, die nicht der Werbung dienen, kann die Rechtsgrundlage wiederum greifen. Dies ist der Fall, wenn die Personalisierung des Inhalts Wesensmerkmal der Dienstleistung ist. Denkbar ist dies z. B. bei Foto-Apps, die auf Grundlage eines hochgeladenen Fotos das Alter des Nutzers schätzen.

Diese Klarstellungen durch den EDSA sind zu begrüßen. Sie fördern die Harmonisierung des Datenschutzrechts und erhöhen das Schutzniveau für die Betroffenen. Schließen doch viele Menschen Verträge in dem Vertrauen ab, dass nichts Untypisches oder gar Überraschendes Vertragsinhalt werden wird. Dies bezieht sich gerade auch auf die damit einhergehenden Datenverarbeitungen.

D. Internationaler Datenverkehr

D.1. Der CLOUD Act – Zugriff von US-Behörden auf Daten in der EU

Die Bedeutung von elektronischem Beweismaterial für Strafverfahren hat in den vergangenen Jahren immens zugenommen. Daher ist der Zugang zu elektronischen Daten für die Strafverfolgungsbehörden elementar. Befinden sich diese Daten im Ausland außerhalb des eigenen Hoheitsgebietes, ist der behördliche Zugriff jedoch nicht ohne weiteres möglich. Der US-CLOUD Act (Clarifying Lawful Overseas Use of Data Act) soll den Zugriff von US-Behörden auf elektronische Daten zur Strafverfolgung erleichtern. Im Juli 2019 nahm der Europäische Datenschutzausschuss (EDSA) Stellung zu diesem US-Gesetz.

Text des CLOUD Act: https://t1p.de/cloudact

Der US-CLOUD Act trat im März 2018 in Kraft und erlaubt US-Behörden, auf personenbezogene Daten zuzugreifen, die im Besitz oder unter der Kontrolle von US-Unternehmen sind – auch dann, wenn sich diese Daten außerhalb der USA befinden. Das Gesetz gilt nur für Anbieter elektronischer Kommunikationsdienstleistungen.

Der direkte Zugriff durch US-Behörden auf Daten außerhalb des US-Hoheitsgebietes ist rechtlich umstritten. Während staatliche Stellen in den USA einen solchen Zugriff bei US-Unternehmen als zulässig ansehen und den CLOUD Act lediglich als Klarstellung verabschiedet haben, betrachtet die EU sämtliche personenbezogenen Daten in ihrem Hoheitsgebiet als durch EU-Recht vor Zugriffen Dritter geschützt. Auch ein US-Gericht hatte einen solchen direkten Zugriff auf personenbezogene Daten eines US-Unternehmens in der EU untersagt.[1]

1 Berufungsentscheidung des Second U.S. Circuit Court of Appeals vom Juli 2016. Die hiergegen gerichtete Beschwerde der US-Regierung wurde im Januar 2017 zurückgewiesen.

Rechtskonflikt mit der DS-GVO

Die Datenschutz-Grundverordnung (DS-GVO) sieht in Art. 48 vor, dass Drittländer per Gerichtsurteil oder Entscheidung von Verwaltungsbehörden von einem europäischen Datenverarbeiter die Übermittlung personenbezogener Daten verlangen können. Allerdings nur dann, wenn hierfür ein Rechtshilfeabkommen zwischen dem Drittland und der EU bzw. einem EU-Mitgliedsstaat vorliegt.

Rechtshilfeabkommen sehen in der Regel einen Austausch der personenbezogenen Daten über zwischengeschaltete staatliche Stellen vor, welche die Rechtmäßigkeit der geplanten Herausgabe prüfen. Eine direkte Herausgabe der Daten an Behörden in Drittländern ist gerade nicht erlaubt. Der Gesetzgeber hat sich mit dieser Regelung in Art. 48 DS-GVO dafür entschieden, ein deutliches Zeichen gegen eine ungeregelte Herausgabe von personenbezogenen Daten aus dem Bereich der EU zu setzen und insbesondere eine Umgehung bestehender Rechtshilfeabkommen zu verhindern.

Unternehmen mit US-amerikanischem Hauptsitz, welche den Regelungen des CLOUD Act unterliegen und Anordnungen von US-Behörden Folge leisten müssen und gleichzeitig als Datenverarbeiter in der EU die Regelung des Art. 48 DS-GVO beachten müssen, befinden sich nun zwangsläufig in einem Rechtskonflikt. Bereits in den Leitlinien 2/2018 zu Einzelfragen des internationalen Datenverkehrs befasste sich der EDSA mit dieser Frage und empfahl betroffenen Unternehmen, sofern eine internationale Übereinkunft besteht, direkte Anfragen zurückzuweisen und die ersuchende Behörde des Drittstaats auf den Weg über bestehende Rechtshilfeabkommen zu verweisen.

Guidelines des EDSA: https://t1p.de/Guidelines

EDSA sieht Bedarf für neues Abkommen

Auch in der europäischen Politik ist der beschriebene Rechtskonflikt wahrgenommen worden: Im März 2019 bat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des EU-Parlaments den EDSA um eine rechtliche Bewertung zu den Auswirkungen des CLOUD Act auf europäisches Datenschutzrecht.

Stellungnahme des EDSA zum CLOUD Act: https://t1p.de/EDSA-CloudAct

Der EDSA hebt in seiner Stellungnahme die Rechtsnorm des Art. 48 DS-GVO hervor, welche gerade das Ziel hat, Datentransfers bzw. -offenlegungen an Behörden in Drittstaaten zu regeln. Der CLOUD Act sei der Versuch, die bestehenden Rechtshilfeabkommen zu umgehen. Demgemäß stellt der EDSA klar, dass die Anforderung einer ausländischen Behörde zur Übermittlung personenbezogener Daten nur dann als rechtliche Verpflichtung des Verantwortlichen nach Art. 6 Abs. 1 lit. c DS-GVO angesehen werden könne, wenn sie auf einem internationalen Abkommen beruhe. Insofern sieht der EDSA Bedarf für ein neues internationales Abkommen zwischen EU und USA, welches hohe datenschutzrechtliche Standards definiert.

Herausgabe nur in sehr engen Grenzen zulässig

Im Übrigen sei eine Herausgabe von personenbezogenen Daten an Behörden eines Drittlandes nur in sehr engen Grenzen zulässig. Der EDSA hält die Übermittlung nur ausnahmsweise für zulässig, wenn außergewöhnliche Umstände vorliegen, etwa zum Schutz lebenswichtiger Interessen einer betroffenen Person (Art. 6 Abs. 1 lit. d i.V.m. Art. 49 Abs. 1 lit. f DS-GVO). Dagegen sieht der EDSA keine Übermittlungsbefugnis aufgrund berechtigter Interessen (Art. 49 Abs. 1 Satz 2 DS-GVO). In der anzustrengenden Interessenabwägung überwiege hier das Schutzinteresse der Betroffenen vor Herausgabe ihrer personenbezogenen Daten, da der Verantwortliche nicht in der Lage sei, die für den Datentransfer vorausgesetzten Garantien für den Schutz der Daten zu geben.

Fazit des EDSA: Eine Herausgabe von personenbezogenen Daten allein auf Grundlage von behördlichen Anforderungen aus den USA auf Basis des CLOUD Act sei in der Regel unzulässig.

Der Rechtskonflikt für die betroffenen Unternehmen bleibt damit zunächst bestehen. Allerdings hat die EU-Kommission 2019 mit den Verhandlungen über ein Abkommen mit den USA begonnen, das die Gewährung eines gegenseitigen Zugangs zu personenbezogenen Daten in Form von elektronischen Beweismitteln beinhalten soll. Aus Sicht des Datenschutzes sollte das Abkommen ausreichende Garantien und Rechtshilfemöglichkeiten für betroffene Personen enthalten.

D.2. Binding Corporate Rules

– Richtlinien für den Datentransfer in Drittländer

Konzerne mit Niederlassungen in mehreren europäischen Ländern und außerhalb der EU nutzen gerne Binding Corporate Rules (BCR) für den internationalen Datentransfer. Dieses Instrument hat durch die Datenschutz-Grundverordnung eine deutliche Aufwertung erfahren. Da die Wirtschaft ein gesteigertes Bedürfnis an einem rechtssicheren Datenaustausch hat, rechne ich mit einer zunehmenden Zahl von Verfahren zur datenschutzrechtlichen Anerkennung von BCR.

Aufsichtsbehörden prüfen BCR

Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules – BCR) einer Unternehmensgruppe sind eine Möglichkeit, Richtlinien zum Umgang mit personenbezogenen Daten als Voraussetzung für einen Datentransfer in das außereuropäische Ausland zu schaffen. Dabei entwickelt das Unternehmen einen eigenen Datenschutzrahmen, der für alle Mitglieder der Unternehmensgruppe Anwendung finden soll. Die Aufsichtsbehörden prüfen zunächst, ob diese eigenen Datenschutzregelungen ein angemessenes Schutzniveau im Sinne der Datenschutz-Grundverordnung (DS-GVO) schaffen und genehmigen nach durchlaufenem Kohärenzverfahren die BCR anschließend. BCR bieten viele Vorteile für Unternehmen, insbesondere da sie anders als etwa die EU-Standardvertragsklauseln auf die besonderen Bedürfnisse der jeweiligen Unternehmen zugeschnitten sind.

Anforderungen der Art. 29-Gruppe übernommen

Die DS-GVO regelt erstmals die Voraussetzungen für die Genehmigung von BCR ausdrücklich. Zuvor waren diese Voraussetzungen in Working Paper der Art. 29-Gruppe (früherer Zusammenschluss der europäischen Aufsichtsbehörden) zusammengefasst. Der Inhalt dieser Working Paper wurde in die DS-GVO übernommen, was eine Weiterführung der inhaltlichen Anforderungen an BCR sichert.

Bindung nach innen und gegenüber Betroffenen

Die DS-GVO legt nun z. B. eindeutig fest, dass die BCR eine rechtliche Bindungswirkung nach innen und gegenüber den betroffenen Personen garantieren müssen. Daneben werden in Art. 47 Abs. 2 DS-GVO inhaltliche Mindestangaben für BCR gesetzlich festgelegt. So müssen etwa die neuen Regelungen der DS-GVO zur Informationspflicht gegenüber den betroffenen Personen, zum Beschwerderecht der Betroffenen und zur Rechenschaftspflicht des Verantwortlichen in die BCR aufgenommen werden. Die DS-GVO schafft damit Rechtssicherheit bezüglich der Anforderungen an BCR in ganz Europa.

EDSA entscheidet über Anerkennung

Eine entscheidende Neuerung betrifft das Verfahren zur Genehmigung von BCR. Nach Art. 63, 64 Abs. 1 DS-GVO entscheidet nun der Europäische Datenschutzausschuss (EDSA) im Kohärenzverfahren über die Anerkennung von BCR. Vor Geltung der DS-GVO genügte die Genehmigung der jeweils für den Verantwortlichen zuständigen Aufsichtsbehörde, welche je nach dem geografischen Anwendungsbereich der BCR die anderen betroffenen Aufsichtsbehörden in der EU beteiligte.[1]

Verfahren wird europaweit vereinheitlicht

Durch die Entscheidung im EDSA wird das Verfahren zur Anerkennung von BCR nun europaweit vereinheitlicht. Auch die entsprechende Genehmigung von konkreten BCR gilt folglich unmittelbar in allen europäischen Mitgliedstaaten. Das Verfahren vor dem EDSA ist gesetzlich genau bestimmt – etwa hinsichtlich der Fristen für bestimmte Verfahrensschritte – und damit auch berechenbarer für das antragstellende Unternehmen.

Da nach neuem Recht über vorgelegte BCR im EDSA entschieden wird, haben sämtliche Aufsichtsbehörden die Gelegenheit, eingebrachte BCR zu prüfen, um eine fundierte Entscheidung treffen zu können. Auch dies trägt zur Vereinheitlichung und zur weiteren Harmonisierung von Datenschutzthemen innerhalb der EU bei. Darüber hinaus erhalten in der Praxis alle Aufsichtsbehörden schon im Vorfeld Gelegenheit zur Stellungnahme und können sich mit Anmerkungen und Kritik zu den vorgelegten BCR beteiligen. Die deutschen Aufsichtsbehörden sind aufgerufen, aktiv an dieser Prüfung teilzunehmen. Daher wird sich auch Niedersachsen künftig stärker in die Diskussion um bestimmte BCR in Europa einbringen.

Beteiligung der LfD Niedersachsen

Eine erste Gelegenheit zur Mitwirkung an einem Prüfungsverfahren nach neuem Recht ergab sich im Jahr 2019 durch die BCR eines Unternehmens mit Hauptsitz in Spanien und einer Niederlassung in Niedersachsen. Das BCR-Verfahren wurde federführend durch die spanische Aufsichtsbehörde betrieben. Niedersachsen beteiligte sich im Rahmen der Co-Prüfung und nahm so Einfluss auf die konkrete Ausgestaltung der BCR.

Erstes Verfahren unter niedersächsischer Federführung

Bereits 2018 stellte ein Unternehmen mit Hauptsitz in Niedersachsen und weltweiten Niederlassungen den Antrag auf Genehmigung der eigenen verbindlichen Datenschutzregelungen. Da die Federführung bei der LfD Niedersachsen lag, konnte meine Behörde sogleich als eine der ersten europäischen Aufsichtsbehörden im neu festgelegten BCR-Verfahren tätig werden. Diese BCR sollen in mehreren europäischen Ländern Geltung erhalten. Meine Behörde überarbeitete den Entwurf gemeinsam mit der italienischen Aufsichtsbehörde, die in diesem Verfahren Co-Prüferin war. Die BCR stehen nun kurz vor der Anerkennung durch den EDSA, womit im ersten Halbjahr 2020 zu rechnen ist.

1 BCR müssen dem EDSA verpflichtend zur Stellungnahme vorgelegt werden. Die Aufsichtsbehörde hat der Stellungnahme des Ausschusses weitestgehend Rechnung zu tragen.

E. DSK

E.1. Hambacher Erklärung zu Künstlicher Intelligenz

Künstliche Intelligenz (KI) ist aktuell das Kernthema der Digitalisierung in Wirtschaft, Wissenschaft und Gesellschaft. Die öffentliche Diskussion um Chancen, Möglichkeiten und Regulierung von KI ist in vollem Gange. Mit der Hambacher Erklärung haben sich die Datenschutzaufsichtsbehörden des Bundes und der Länder in diese Diskussion eingebracht und die Berücksichtigung der DS-GVO beim Einsatz von KI-Systemen gefordert.

Ob automatisierte Fahrzeuge, Sprachassistenten, Krebsprävention oder Gesichtserkennung: Künstliche Intelligenz ist eine Schlüsseltechnologie, mit der häufig personenbezogene Daten verarbeitet und Entscheidungen getroffen werden, die für die Betroffenen erhebliche Auswirkungen haben können. Die Datenschutzaufsichtsbehörden sind daher gehalten, sich frühzeitig mit dieser Technologie, ihren Chancen und Risiken für die Menschen auseinanderzusetzen. Dementsprechend hat die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (DSK) eine Arbeitsgruppe zum Thema „Datenschutzanforderungen an auf künstliche Intelligenz gestützte Datenverarbeitungen“ eingesetzt, an der sich mein Haus aktiv beteiligt.

Anforderungen an den KI-Einsatz

Überhaupt hat die DSK 2019 diesem Zukunftsthema einen besonderen Stellenwert eingeräumt. Als zentrales Dokument verabschiedete sie am 3. April 2019 im Rahmen der 97. Datenschutzkonferenz die „Hambacher Erklärung zur künstlichen Intelligenz“.

Hambacher Erklärung:
https://t1p.de/hambacher

Diese Erklärung enthält sieben datenschutzrechtliche Anforderungen an KI-Systeme, die sich aus der DS-GVO ergeben:

1. KI darf Menschen nicht zum Objekt machen
2. KI darf nur für verfassungsrechtlich legitimierte Zwecke eingesetzt werden und das Zweckbindungsgebot nicht aufheben

3. KI muss transparent, nachvollziehbar und erklärbar sein
4. KI muss Diskriminierungen vermeiden
5. Für KI gilt der Grundsatz der Datenminimierung
6. KI braucht Verantwortlichkeit
7. KI benötigt technische und organisatorische Standards

Es steht außer Frage, dass wirtschaftliche und gesellschaftliche Chancen, die sich aus der technischen Entwicklung im Bereich künstlicher Systeme ergeben, genutzt werden sollen. Allerdings müssen gerade bei der Entwicklung und Verbreitung dieser Technologien, die in weiten Teilen einen geradezu disruptiven Charakter besitzen, die Grundrechte der Bürgerinnen und Bürger gewahrt werden. Dies stellt alle Beteiligten vor eine gewaltige Herausforderung.

#Künstliche Intelligenz

1

Künstliche Intelligenz
| *Artificial Intelligence*

Teilgebiet der Informatik mit dem Ziel, Maschinen/ Programme zu befähigen, Aufgaben intelligent auszuführen

2

Maschinelles Lernen
| *Machine Learning*

Algorithmen, die anhand von Beispielen Merkmale der Daten erlernen. Das gelernte „Modell" kann dann genutzt werden, **um Aufgaben der künstlichen Intelligenz zu erfüllen**.

1. Algorithmus lernt Merkmale
2. Algorithmus entwickelt abstrakte Merkmale und ein Modell
3. Algorithmus überprüft abstrakte Merkmale und passt sie ggf. an

3

Tiefes Lernen
| *Deep Learning*

Methode des Maschinellen Lernens

- arbeitet mit **künstlichen neuronalen Netzen** KNN (nach dem Vorbild des menschlichen Gehirns)
- KNN lernen durch die Analyse großer Datenmengen

13081 © **Globus** Quelle: Fraunhofer Institut, Spektrum.de

Empfehlungen für Entwicklung und Betrieb

Positionspapier zu KI-Systemen: https://t1p.de/position-ki

Um die datenschutzrechtlichen Anforderungen weiter zu konkretisieren, veröffentlichte die DSK am 6. November 2019 ein Positionspapier. Dieses enthielt empfohlene technische und organisatorische Maßnahmen für Entwicklung und Betrieb von KI-Systemen.

Strukturell durchlaufen KI-Systeme verschiedene Phasen,
die aufeinander aufbauen:

1. Design des KI-Systems und der KI-Komponenten
2. Veredelung der Rohdaten zu Trainingsdaten
3. Training der KI-Komponenten
4. Validierung der Daten und KI-Komponenten sowie angemessene Prüfungsmethoden
5. Einsatz und Nutzung des KI-Systems
6. Rückkopplung von Ergebnissen und Selbstveränderung des Systems.

In allen Phasen werden in der Regel in unterschiedlichem Umfang und zu unterschiedlichen Zwecken (personenbezogene) Daten verarbeitet. Daher wurden die bewährten Gewährleistungsziele des Datenschutzes typischen Entwicklungsphasen eines KI Systems zugeordnet. Nur so ist von vornherein gewährleistet, dass bereits im technischen Design eine verhältnismäßige und wirksame Wahrung der Grundrechte der Bürgerinnen und Bürger implementiert wird.

Die Gewährleistungsziele im Datenschutz sind:

- Datenminimierung
- Transparenz
- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Nicht-Verkettbarkeit
- Intervenierbarkeit

SDM abrufbar unter: https://t1p.de/sdm2

Auf Basis des Standard-Datenschutzmodells in der Version 2.0 (SDM) (siehe auch J.12.1, S. 189) wurden in dem Positionspapier abgesehen von der Zuordnung der Gewährleistungsziele zu den einzelnen Phasen eines KI-Systems besonders die jeweiligen Maßnahmen beschrieben, die bei einem datenschutzkonformen Einsatz von KI-Systemen zu berücksichtigen sind. Aufgrund der großen Dynamik, die die Weiterentwicklung der KI derzeit entfaltet, wird sich mein Haus auch weiterhin intensiv mit den Modellen und Lösungen zur Künstlichen Intelligenz befassen.

E.2. Arbeitskreise der DSK

– Fokus auf Versicherungen und Beschäftigte

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) deckt ein breites Spektrum von Themen ab. Unterstützt wird sie dabei von ihren 26 Arbeitskreisen. Diese sollen der DSK zuarbeiten, ihre Entscheidungen vorbereiten und deren Aufträge umsetzen. In zwei dieser Gremien hatte meine Behörde im vergangenen Jahr den Vorsitz inne.

Arbeitskreise der DSK: https://t1p.de/dsk-ak

Zum einen führt die LfD Niedersachsen seit April 2016 den Vorsitz im Arbeitskreis (AK) Beschäftigtendatenschutz. Ziel dieses AK ist es, einheitliche Positionierungen aller Aufsichtsbehörden zu datenschutzrechtlichen Fragen im Beschäftigtenkontext zu erarbeiten.

Darüber hinaus ist es Aufgabe des AK Beschäftigtendatenschutz, anderen Gremien der DSK bei Fragen aus diesem Themenbereich zuzuarbeiten. So gab der AK eine Stellungnahme zur „Orientierungshilfe zur Aufbewahrung von Geschäftsunterlagen durch externe Dienstleister" ab. Hier ging es um die Frage, ob von den mit der Archivierung betrauten Beschäftigten des Dienstleisters die Vorlage eines (allgemeinen) Führungszeugnisses verlangt werden kann, um deren Zuverlässigkeit zu klären. Die Abstimmung über die Orientierungshilfe auf DSK-Ebene war zum Ende des Berichtszeitraums noch nicht abgeschlossen.

Austausch zu Praxisfragen

Zudem dient der Arbeitskreis dem Erfahrungsaustausch der Behörden. Dieses ist in der Praxis insbesondere bei Datenschutzüberprüfungen nach der Datenschutz-Grundverordnung (DS-GVO) sehr hilfreich. Neben dem Austausch über aktuelle Entwicklungen – etwa zur Verwendung biometrischer Daten – werden auch konkrete praxisorientierte Fragen aus dem Tätigkeitsfeld der nationalen und europäischen Datenschutzaufsichtsbehörden erörtert.

Rechtsfragen zur Umsetzung der DS-GVO

So behandelte der AK Beschäftigtendatenschutz 2019 eine Vielzahl von Sachthemen von „A", wie „Abfrage von Beschäftigtendaten" bis „Z", wie „Zeiterfassung". Auch Rechtsfragen im Zusammenhang mit der Umsetzung der DS-GVO wurden behandelt: zum Beispiel die Reichweite des Rechts auf Erhalt einer Kopie von Personalakten nach Artikel 15 Absatz 3 und 4 DS-GVO, die Ausgestaltung von Dienst- oder Beschäftigtenausweisen oder die Frage der Verantwortlichkeit von Interessenvertretungen.

AK Versicherungswirtschaft

Die Versicherungsbranche verarbeitet in besonders großem Umfang personenbezogene Daten, darunter auch eine Vielzahl von Daten besonderer Kategorien. Vor diesem Hintergrund ist diese Branche ein gewichtiger Faktor in der Arbeit der LfD Niedersachsen. Darüber hinaus ist die Versicherungsbranche auch ein bedeutsamer Teil der niedersächsischen Wirtschaft insgesamt. Deshalb hat sich die LfD Niedersachsen einer neuen Aufgabe gestellt und Anfang 2019 den Vorsitz des Arbeitskreises Versicherungswirtschaft übernommen. Die erste Sitzung dieses AK unter niedersächsischer Leitung fand im September in Hannover statt.

Schwerpunkte: Muster und Codes of Conduct

Neben allgemeinen datenschutzrechtlichen Fragestellungen, wie Informationspflichten, Auskunftsrecht und Löschfristen, wurden 2019 im AK vor allem folgende Themen diskutiert:

Der Gesamtverband der Versicherungswirtschaft (GDV) legte dem AK Versicherungswirtschaft neue, an die DS-GVO angepasste Muster zur Einwilligungs- und Schweigepflichtentbindungserklärung vor. Diese wurden im Rahmen der ersten Sitzung unter niedersächsischer Leitung vom AK eingehend erörtert. Da noch Klärungs- und Anpassungsbedarf gesehen wurde, bildete der AK eine Unterarbeitsgruppe, die sich in den folgenden Monaten intensiv mit den Mustern auseinandersetzen wird.

Darüber hinaus strebt der AK eine Finalisierung der Verhaltensregeln (Codes of Conduct, CoC) der Versicherungswirtschaft durch den GDV an. Diese ist gemäß Art. 40 DS-GVO Voraussetzung für die Genehmigung. Dem GDV wurde mitgeteilt, dass für die Genehmigung eines CoC die Einrichtung einer Kontrollstelle aus Sicht des AK zwingende Voraussetzung ist. Diese Sicht basiert auf den vom Europäischen Datenschutzausschuss (EDSA) verabschiedeten Leitlinien zu CoC („Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies unter Regulation 2016/679“[1]). Hier hatte der AK zunächst die grundsätzliche Klärung auf europäischer Ebene abgewartet.

Guidelines des EDSA:
https://t1p.de/Guidelines

1 in der Version vom 21.05.2019 (nach der öffentlichen Konsultation)

E.3. Gesetzesänderung zur Meldepflicht von Datenschutzbeauftragten

Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten. sorgt seit Geltung der DS-GVO immer wieder für Diskussionen. Im April 2019 sprachen sich die deutschen Aufsichtsbehörden in einer Entschließung der Datenschutzkonferenz (DSK) gegen eine Verwässerung der nationalen Regelungen aus. Dennoch trat am 26. November 2019 eine Gesetzesänderung in Kraft, die vorsah, dass Unternehmen und Vereine erst dann einen Datenschutzbeauftragten bestellen müssen, wenn dort 20 oder mehr Personen regelmäßig personenbezogene Daten elektronisch verarbeiten. Zuvor lag die Grenze bei 10 Personen.

Entschließung der DSK: https://t1p.de/dsk-dsb

Die Änderung zur Bestellpflicht des Datenschutzbeauftragten (DSB) war Teil des Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU, dem der Bundesrat am 20. September 2019 zustimmte. Seit Inkrafttreten des Gesetzes müssen – über die besonderen Fälle der Datenschutz-Grundverordnung (DS-GVO) und des Bundesdatenschutzgesetzes (BDSG) hinaus – nur Unternehmen einen DSB benennen, die in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.

Anforderungen bleiben auch ohne DSB bestehen

Unternehmen, die zwischen 10 und 20 Beschäftigte in der Verarbeitung personenbezogener Daten einsetzen, werden dies zunächst als Erleichterung wahrnehmen. Die Gesetzesänderung bedeutet aber nicht, dass die Vorgaben des Datenschutzrechts nicht einzuhalten wären. In ihrer Entschließung hatte die DSK bereits im April festgestellt: „Die Datenschutzbeauftragten sorgen für eine kompetente datenschutzrechtliche Beratung, um Datenschutzverstöße (…) zu vermeiden und das Sanktionsrisiko gering zu halten. (…) Der Wegfall mag kurzfristig als Entlastung empfunden werden. Mittelfristig geht interne Kompetenz verloren."

Die betroffenen Unternehmen sollten deshalb erwägen, unabhängig von der Gesetzesänderung, ihren DSB weiter zu beschäftigen, um das datenschutzrechtliche Know-how für ihr Unternehmen aufrecht zu erhalten und weiter aufzubauen. Nach Artikel 37 Absatz 4 DS-GVO kann der Verantwortliche einen DSB benennen, auch wenn er nicht aufgrund anderer gesetzlicher Vorgaben dazu verpflichtet ist.

Empfehlung: DSB weiter beschäftigen

Darüber hinaus weise ich darauf hin, dass die neue Gesetzeslage weder ein Sonderkündigungsrecht für bestehende DSB-Dienstleistungsverträge beinhaltet, noch eine ordnungsgemäße Benennung ihre Gültigkeit verliert.

Die weiteren gesetzlichen Regelungen zur Benennungspflicht in § 38 BDSG und Artikel 37 DS-GVO bleiben von der Gesetzesänderung unberührt.

E.4. Registermodernisierung

– Diskussionen um Daten in der digitalen Verwaltung

Die Bundesregierung plant eine Modernisierung der Registerlandschaft in Deutschland. Im März 2019 setzte der IT-Planungsrat[1] das Koordinierungsprojekt „Registermodernisierung" auf, um dafür Leitlinien abzustimmen. Teil der Debatte ist auch die Einführung einer einheitlichen Personenkennziffer.

„Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren." Laut diesem Gutachten des Nationalen Normenkontrollrats (NKR) stehen bei der Registermodernisierung drei Ziele im Vordergrund:

1. Verwaltungsleistungen für Bürger und Unternehmen digitalisieren,
2. die Datengrundlage für staatliche Entscheidungen und amtliche Statistiken verbessern sowie
3. den Zugriff auf staatliche Daten für die Wirtschaft erleichtern.

Chancen und Risiken in Ausgleich bringen

Mit dem Gutachten des NKR erreichte die Debatte um die Einführung einer Personenkennziffer in Deutschland 2017 einen neuen Höhepunkt. Es gilt, die Chancen einer effizienteren Verwaltung durch die intensivere Vernetzung von Daten und die Risiken für die Freiheitsrechte und die informationelle Selbstbestimmung der Bürger in einen angemessenen Ausgleich zu bringen.

Der Weg zur optimalen und sicheren Nutzung der Daten in einer digitalisierten Verwaltung scheint noch weit zu sein. Deutschland landet im internationalen Vergleich bei E-Government laut Gutachten auf einem der hinteren Plätze.[2] Es wäre ein Gewinn, wenn Bürgerinnen und Bürger durch eine Registermodernisierung mehr serviceorientierte Dienstleistungen des öffentlichen Bereichs nutzen könnten. Dieser Mehrwert darf allerdings nicht zu Lasten des Datenschutzes gehen.

1 Koordinierungsgremium zur Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik

2 Gutachten des Normenkontrollrats „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren." vom Oktober 2017

Chancen der Digitalisierung besser nutzen

Klar ist: Damit Deutschland auch künftig über eine zeitgemäße und gute Verwaltung verfügt, müssen die Chancen der Digitalisierung besser genutzt werden. In seinem Gutachten beschreibt der Normenkontrollrat, dass die Modernisierung der Registerlandschaft Grundlage der Digitalisierung der öffentlichen Verwaltung sein muss. Moderne Register seien essenziell für effiziente, bürger- und unternehmensfreundliche digitale Angebote.

Häufig genutzte Daten sollen zentral gespeichert werden

Die Innenministerkonferenz beschloss im Juni 2019, ein registerübergreifendes Identitätsmanagement als wesentlichen Bestandteil der Registermodernisierung aufzubauen. Das soll die eindeutige Zuordnung einer Personenidentität über alle Register hinweg sicherstellen. Häufig genutzte Basisdaten zu einer Person sollen zentral an einer Stelle gespeichert werden. Um den Datenaustausch zu einer Person behördenübergreifend zu verbessern und Verwechselungen weitestgehend auszuschließen, soll eine eindeutige Identifikation dieser Person möglich werden.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben frühzeitig eine Kontaktgruppe gebildet, die in unterschiedlichen Arbeitsgruppen beratend mitarbeitet, um die Initiativen der Bundesregierung aus datenschutzrechtlicher Sicht zu begleiten.

DSK lehnt übergreifende Personenkennzeichen ab

DSK zur digitalen Verwaltung: https://t1p.de/verwaltung-digital

In ihrer im September 2019 veröffentlichten Entschließung „Digitalisierung der Verwaltung datenschutzkonform und bürgerfreundlich gestalten!“ fordert die DSK ausreichende datenschutzrechtliche Garantien bei der Umsetzung der Registermodernisierung. Nach Auffassung der DSK muss die Verbesserung der staatlichen Dienstleistungen mit ausreichenden datenschutzrechtlichen Garantien einhergehen.

Mit der Registermodernisierung wird auch eine nutzerfreundliche Umsetzung des Onlinezugangsgesetzes (OZG) verfolgt. Einmal vom Bürger hinterlegte Daten sollen auch von anderen Verwaltungen genutzt werden können. Damit der Bürger die notwendige Transparenz erhält, fordert die DSK in ihrer Entschließung ein Datencockpit. Dieses Cockpit soll den Bürgerinnen und Bürgern erlauben, jederzeit nachzuvollziehen, welche Behörden Daten über sie vorhalten und welche Behörden diese nutzen.

Alternative Methoden zur Identifizierung gefordert

Allerdings lehnt die DSK die Nutzung von einheitlichen, verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren zur direkten Identifizierung von Bürgerinnen und Bürgern ab. Aus Sicht der Datenschutzkonferenz sind allenfalls sektorspezifische Personenkennziffern verwendbar, die eine eindeutige Identifizierung erlauben, den einseitigen Abgleich von Daten verhindern, das Risiko von Missbrauch und Kompromittierung verringern sowie die Eindeutigkeit von Registern gewährleisten. Die DSK fordert alternative Methoden zur eindeutigen Identifizierung.

Mit dieser Forderung nach bereichsspezifischen Kennziffern soll auch dem Prinzip des Datenschutzes durch Gestaltung (Data protection by Design) Rechnung getragen werden, welches durch die DS-GVO eine größere Bedeutung erlangt hat. Es ist mir besonders wichtig, dass bei dieser Neuentwicklung Datenschutzanforderungen von Anfang an mitberücksichtigt werden. Meine Behörde arbeitet deshalb in der oben erwähnten Kontaktgruppe mit.

E.5. Doxxing

– DSK reagiert auf Datenlecks

Am 3. Januar 2019 berichteten verschiedene Medien, dass Unbekannte teils sehr persönliche Informationen von hunderten deutschen Politikern, Künstlern und anderen Personen des öffentlichen Lebens veröffentlicht hatten. Nur wenige Wochen später kam ein noch größeres Datenleck ans Licht. Die Ereignisse warfen einmal mehr ein Schlaglicht auf die Bedeutung des Schutzes von Zugangsdaten und veranlassten die Konferenz der Aufsichtsbehörden zu einer Reaktion.

Im Fall von Anfang Januar 2019 handelte es sich um das so genannte „Doxxing". Der Begriff Doxing oder auch Doxxing leitet sich von „dox" als Kurzform des englischen „documents" ab. Er bezeichnet das internetbasierte Zusammentragen und anschließende Veröffentlichen personenbezogener Daten.

Was ist Doxxing?

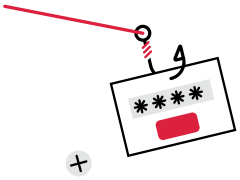
Das Veröffentlichen persönlicher Daten – gegen den Willen des Betroffenen.

So funktioniert Doxxing

Doxx vom englischen Begriff documents (Dokumente)

1. Sammeln von privaten Daten, z. B. über ...

Phishing Trojaner wird per E-Mail an Betroffenen gesendet: Fremder erhält unbemerkt Kontrolle über Gerät; greift z. B. Passwörter von E-Mail-Accounts, sozialen Netzwerken ab. Durchstöbern des Geräts nach sensiblen Daten wie Telefonnummern, Fotos oder Chatverläufen.



Hackerangriff Angreifer nutzt Sicherheitslücke aus, um z. B. auf Server einer Firma zu gelangen und massenhaft Kreditkartennummern o. Ä. abzugreifen.

Social Engineering Fremder gibt sich als jemand anderes aus, um über Dritte an persönliche Daten des Ausspionierten zu gelangen, etwa an Handynummer.

Durchsuchen **öffentlicher Datenbanken** nach persönlichen Infos wie Adressen, Rufnummern.

2. Gesammelte Daten werden im Internet gespeichert.

3. Veröffentlichen der Daten

dpa•29608 Quelle: dpa

Unsichere Passwörter noch immer weit verbreitet

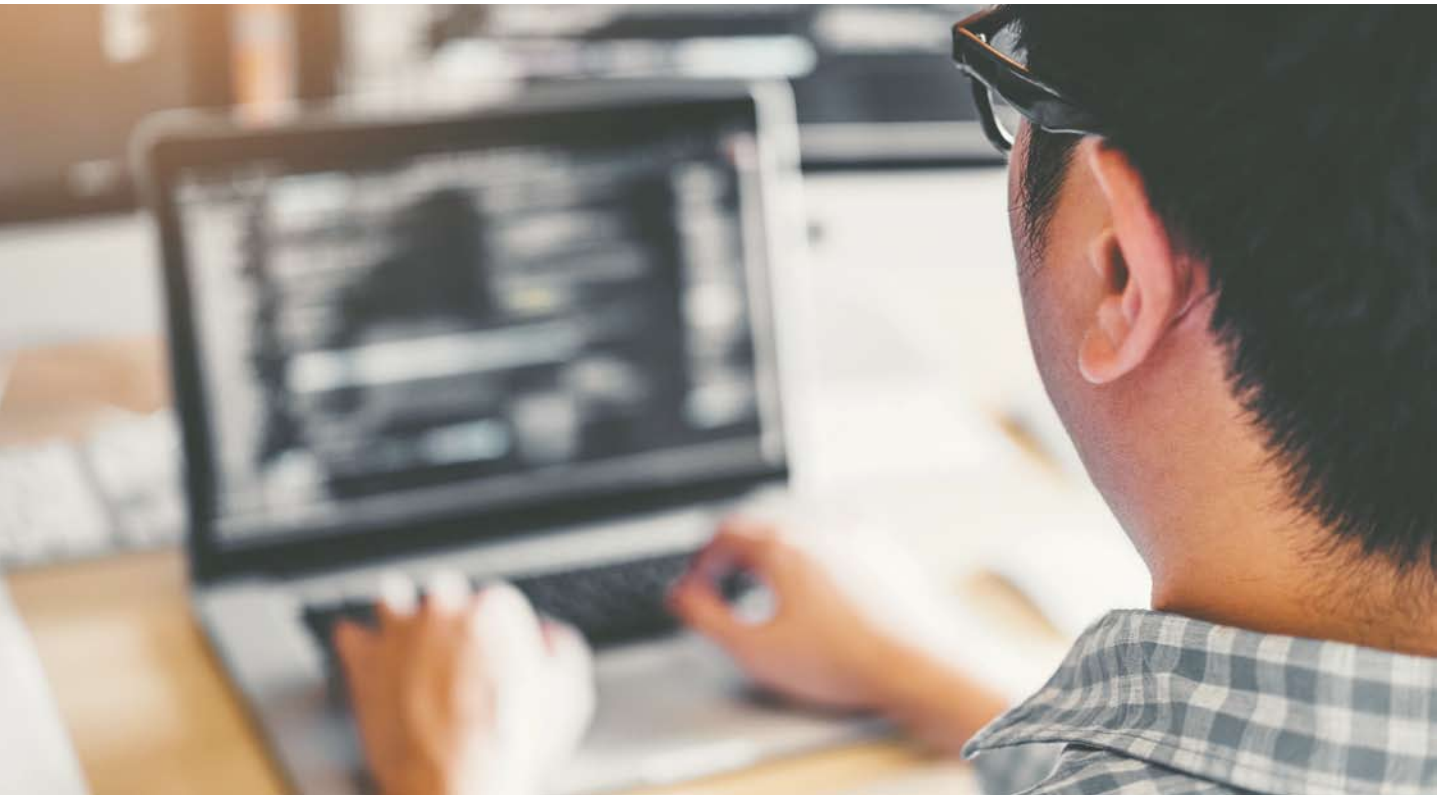
Nach Ansicht des Bundeskriminalamtes waren schlechte Passwörter die Hauptursache dieser massenhaften Datendiebstähle. Nach der Erfahrung meiner Behörde ist es noch immer sehr verbreitet, schlechte, also leicht zu erratende bzw. zu überwindende Passwörter zu nutzen. Zudem hat sich bei der Anmeldung zu Online-Diensten noch nicht überall ein zweiter Authentisierungsfaktor (z. B. eine mTan) als zusätzliche Sicherheitshürde durchgesetzt. Dies führt dazu, dass Zugangsdaten zu leicht missbraucht werden können. Im Zusammenhang mit diesem Doxxing-Vorfall stellte sich zudem einmal mehr Frage, inwieweit auch Diensteanbieter, Behörden und nicht-öffentliche Stellen als die Verantwortlichen der Datenverarbeitung ihre Sicherheitslösungen angemessen und datenschutzkonform umsetzen und damit zu einem hinreichenden Schutzniveau beitragen.

DSK veröffentlicht Orientierungshilfe

Nur wenig später gelangte ein noch weitaus größeres Datenleck an die Öffentlichkeit. Unter dem Namen Passwort-Leaks wurde Ende Januar 2019 bekannt, dass 2,2 Milliarden gehackte Nutzer-Accounts ins Netz gelangt seien – eine völlig neue Dimension der Verletzung von Rechten und Freiheiten der betroffenen Personen.

Orientierungshilfe zum Download: https://t1p.de/oh-online

Auf einer Zwischenkonferenz der unabhängigen Aufsichtsbehörden des Bundes und der Länder (DSK) im Januar 2019 wurde der Vorfall beraten. Das Ergebnis: Der Arbeitskreis (AK) Technik erhielt den Auftrag, eine Orientierungshilfe für Anbieter elektronischer Dienste zu erstellen. In dieser sollten Empfehlungen zusammengestellt werden, mit denen ein angemessener Schutz von Zugangsdaten erreicht werden kann. Der AK Technik veröffentlichte die Orientierungshilfe im März 2019 unter dem Titel „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“.



Die Ursachen der beiden Datenschutzverletzungen müssen natürlich einzeln betrachtet werden, um alle Umstände identifizieren zu können. So ist es im Fall des Doxxings nicht ausgeschlossen, dass auch Fehler beim Selbstdatenschutz der Betroffenen gemacht wurden, etwa durch unsichere Passwörter oder die Einstellungen der eigenen Betriebssysteme. Dagegen scheinen bei Passwort-Leaks, als komplette Authentifizierungsdatenbanken von Servern im Internet kursierten, die Dienstanbieter Urheber des Problems zu sein.

Problem systematisch angehen

Angesichts dieser unterschiedlichen Ursachen möglicher Szenarien konnte die Orientierungshilfe der DSK keine abschließende Liste mit Mindestanforderungen oder gar komplette Anleitungen für mehr Datenschutz enthalten. Zielführender erschien eine nicht abschließende Maßnahmenliste, die an die Problemlösung systematisch herangeht. Sie soll Hinweise zu Methoden und Technologien beinhalten, die sich aus Sicht der Aufsichtsbehörden bewährt haben.

Verantwortliche müssen bei der Auswahl der individuell geeigneten technischen und organisatorischen Maßnahmen den risikobasierten Ansatz, wie er durch Artikel 32 Abs. 1 DS-GVO vorgegeben ist, zugrunde legen. Sie müssen demnach

- den Stand der Technik,
- die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung (im Sinne des Art. 4 lit. 2 DS-GVO),
- die Implementierungskosten sowie
- die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen

berücksichtigen, um ein diesem Risiko angemessenes Schutzniveau zu gewährleisten.
Damit ergeben sich zwar grundsätzliche Mindestanforderungen für die Authentisierung und Authentifizierung. Die jeweilige Lösung ist allerdings vom individuellen Verarbeitungskontext und dem daraus resultierenden Schutzniveau abhängig.

Empfehlungen zu Passwörtern aktualisiert

Ergänzend zur Orientierungshilfe des AK Technik hielt ich es für notwendig, meine bisherigen Passwortempfehlungen zu aktualisieren. Daher veröffentlichte ich im August eine neue „Handlungsempfehlung sichere Authentifizierung“ welche sich an Nutzer, Verantwortliche und Dienstleister richtet.

Handlungsempfehlung zur sicheren Authentifizierung: https://t1p.de/handlung-passwoerter

Verantwortliche sollten unter Beachtung dieser beiden Hilfestellungen Daten, Verarbeitungsprozesse, Infrastruktur und Systeme einer systematischen Analyse unterziehen und ihre Maßnahmen ggf. nachbessern. Dieser Prozess muss regelmäßig wiederholt werden, um IT-Produkte jederzeit auf der Grundlage aktualisierter Analysen weiterzuentwickeln.

Die Nutzerinnen und Nutzer von Services, Websites, Geräten und Apps sollten bei der Wahl ihrer Produkte die Einhaltung der in den beiden Hilfestellungen beschriebenen Kriterien durch die Anbieter zugrunde legen. Tun sie das, hätten letztlich nur noch sichere Lösungen eine Marktchance und veraltete und unsichere Produkte würden vom Markt verschwinden.

E.6. Office 365 – datenschutzkonformer Einsatz möglich?

Die Anwendungen von Office 365 sind sowohl in öffentlichen als auch nicht-öffentlichen Stellen weit verbreitet. Die Datenschutzkonferenz prüft derzeit, ob ein datenschutzkonformer Einsatz der Microsoft-Produkte möglich ist.

Verantwortliche Datenverarbeiter traten im Berichtszeitraum vermehrt an mich mit der Frage heran, ob sie Office 365 datenschutzkonform einsetzen können. Hintergrund ist häufig der Wunsch der Verantwortlichen, die Cloud-Funktionen zu nutzen. Allerdings lässt sich diese Frage nicht pauschal beantworten.

DSK setzt Arbeitskreis ein und führt Gespräche mit Microsoft

Da die Unsicherheiten zum Einsatz von Microsoft Office 365 nicht nur mir, sondern allen Landesbeauftragten in Deutschland kommuniziert wurden, entschloss sich die Konferenz der unabhängigen Aufsichtsbehörden (DSK) einen Arbeitskreis (AK) einzusetzen, der sich unter Beteiligung meiner Behörde mit dieser Frage befasst. Auch mit Vertretern von Microsoft wurden in diesem Zusammenhang Gespräche geführt, in denen verschiedene Fragen von Bedeutung waren.

Online Service Terms auf dem Prüfstand

Zunächst handelt es sich bei der Nutzung der Cloud eines Dritten regelmäßig um einen Fall der Auftragsverarbeitung. Daher müssen die Anforderungen des Art. 28 DS-GVO erfüllt sein und ein Vertrag zur Auftragsverarbeitung geschlossen werden. Eine entsprechende Vereinbarung wird den Kunden von Microsoft in einer standardisierten Form mit den Online Services Terms (OST) angeboten. Nach erster Prüfung dieser Vereinbarung durch den AK ergab sich eine Reihe von Fragen, zu denen der AK noch mit Microsoft im Dialog steht. Die Prüfung konnte daher 2019 nicht abgeschlossen werden. Zudem hat Microsoft angekündigt, Anfang 2020 seinen Kunden eine neue Version der OST zur Verfügung stellen zu wollen. Zum Ende des Berichtszeitraums war noch unklar, inwieweit die Anregungen der Datenschutzkonferenz darin aufgegriffen und die Regelungen zur Auftragsverarbeitung angepasst wurden.

Darüber hinaus stellt sich auch bei Office 365 – ähnlich wie bei Windows 10 (siehe dazu auch J.12.3, S. 193) – die Frage nach dem Inhalt und der Rechtmäßigkeit der Übermittlung von Telemetriedaten, die zu Servern von Microsoft übermittelt werden. Dazu gehören beispielsweise Daten zu Abstürzen, zum CPU- und Speicherverbrauch einzelner Programme, Daten zum Prozessor, In-

formationen zum Akkustand oder zu Downloads, Updates, und Abrufen im Windows App Store. Nach Angaben des Unternehmens werden diese Daten dazu verwendet, um Office 365 aktuell und sicher zu halten, Probleme zu erkennen und zu beseitigen und die Produkte zu verbessern.[1] Das von der DSK veröffentlichte Prüfschema zum Einsatz von Windows 10 dürfte entsprechend auch auf Office 365 anwendbar sein. Nach der Prüfung der OST wird sich die DSK auch bei Office 365 mit dem Thema der Telemetriedaten befassen.

Prüfschema Windows 10: https://t1p.de/Pruefschema-Windows10

Mir ist bewusst, dass die Verantwortlichen bei der datenschutzrechtlichen Beurteilung dieser Standard-Software Rechtssicherheit benötigen. Ich bin zuversichtlich, dass die DSK sich hierzu 2020 positionieren kann.

1 https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data

E.7. Kritik an Änderung des Rundfunkbeitrags-Staatsvertrags

Im Berichtszeitraum wurde ein Referentenentwurf zur Änderung des Rundfunkbeitrags-Staatsvertrags veröffentlicht. Eine Regelung des Entwurfs sah vor, dass alle vier Jahre Meldedaten sämtlicher volljähriger Personen an die jeweils zuständige Landesrundfunkanstalt übermittelt werden. Damit sollte die Aktualität des dortigen Datenbestandes sichergestellt werden. Die unabhängigen Datenschutzaufsichtsbehörden veröffentlichten dazu einen kritischen Beschluss.

Zu den Meldedaten, die im Abgleich übermittelt werden sollen, zählen neben Namen, gegenwärtiger und letzter Anschrift sowie dem Geburtsdatum auch Titel, Familienstand und die genaue Lage der Wohnung. Die Datenschutzkonferenz (DSK) reagierte auf den Referentenentwurf mit dem Beschluss „Geplante Einführung eines regelmäßigen vollständigen Meldedatenabgleichs zum Zweck des Einzugs des Rundfunkbeitrags stoppen“ vom 26. April 2019. Darin betont sie, dass bereits gegen die in den Jahren 2013 und 2018 durchgeführten vollständigen Meldedatenabgleiche erhebliche datenschutzrechtliche Bedenken bestanden hatten. Die DSK hatte damals ihre Bedenken nur deshalb teilweise zurückgestellt, weil lediglich ein einmaliger Abgleich vorgenommen werden sollte, um den Start in das neue Beitragsmodell zu erleichtern.

Beschluss der DSK: https://t1p.de/meldeabgleich

Trotz der eindeutigen Stellungnahme der DSK wurde der 23. Rundfunkänderungs-Staatsvertrag, der die Änderung des Rundfunkbeitrags-Staatsvertrags umfasst, von der Ministerpräsidentenkonferenz am 25. Oktober 2019 unterzeichnet. Er soll zum 1. Juni 2020 in Kraft treten.

Staatskanzlei lässt LfD Niedersachsen außen vor

Ich habe erhebliche verfassungsrechtliche Bedenken gegen den damit eingeführten regelmäßigen vollständigen Meldedatenabgleich und sehe in den konkreten Regelungen einen massiven Verstoß gegen die Grundsätze des Datenschutzrechts. Zudem möchte ich darauf hinweisen, dass die Niedersächsische Staatskanzlei es unterlassen hat, mich vor der Unterzeichnung des 23. Rundfunkänderungs-Staatsvertrag ordnungsgemäß zu beteiligen. Dies schränkt meine Möglichkeiten erheblich ein, mich für die Belange der Bürgerinnen und Bürger zur Durchsetzung ihrer informationellen Selbstbestimmung im erforderlichen Maße einsetzen zu können.

Massiver Verstoß gegen Grundsätze des Datenschutzes

E.8. Orientierungshilfe:
Spielregeln für das Webtracking

Die Datenschutz-Grundverordnung (DS-GVO) sorgte bei Webseiten-Betreibern für viele Unsicherheiten zum Webtracking. Neben der Frage, ob auch unter Geltung der DS-GVO das Telemediengesetz (TMG) noch anwendbar sei, war zu klären, welche Vorgänge überhaupt unter das Webtracking fallen und wie die Einwilligung eines Nutzers zum Tracking gestaltet und eingebunden werden muss. Die Aufsichtsbehörden gaben in einer Orientierungshilfe Antworten.

Im März 2019 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) die „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien". Sie ergänzte die am 26. April 2018 veröffentlichte „Positionsbestimmung zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018". Nach der Veröffentlichung der Positionsbestimmung hatte die DSK eine Konsultation von betroffenen Wirtschaftsverbänden und Unternehmen zum Webtracking durchgeführt. Die Orientierungshilfe berücksichtigt die Stellungnahmen im Konsultationsverfahren und dient der Konkretisierung der Positionsbestimmung.

Informationen und Downloads zum Webtracking: https://t1p.de/web-tracking

Im ersten Teil der Orientierungshilfe wird umfassend begründet, warum die §§ 11 ff. des TMG seit der Geltung der DS-GVO nicht mehr anwendbar sind. Daraus folgt, dass die datenschutzrechtliche Bewertung des Webtrackings in Deutschland ausschließlich auf Grundlage des DS-GVO vorzunehmen ist. Anschließend werden im zweiten Teil ausführliche Hinweise für die Prüfung der Rechtmäßigkeit des Webtrackings erteilt und durch zahlreiche Beispiele verdeutlicht.

Kriterien für Interessensabwägung

Die Orientierungshilfe stellt insbesondere klar, dass

- nicht jeglicher Einsatz von Cookies einwilligungsbedürftig ist und
- die Verarbeitung personenbezogener Daten in Zusammenhang mit der Nutzung von Webseiten von Unternehmen grundsätzlich aufgrund Einwilligung, Vertrag oder berechtigter Interessen des Verantwortlichen rechtmäßig sein kann (Art. 6 Abs. 1 lit. a, b und f DS-GVO).

Orientierungshilfe https://t1p.de/oh-telemedien

Des Weiteren enthält sie ein Schema für die Prüfung der Voraussetzungen von Art. 6 Abs. 1 lit. f DS-GVO und nennt Kriterien, die bei der erforderlichen Interessenabwägung zu berücksichtigen sind.

Nach meiner Wahrnehmung wird die Orientierungshilfe in der Praxis sehr gut angenommen. Sofern es die Kapazitäten in meiner Behörde erlauben, werde ich besonders im Bereich Internet und mobile Apps verstärkt weitere praxisorientierte Präventionsarbeit leisten.

F. Rechtsprechung von grundsätzlicher Bedeutung

F.1. EuGH entscheidet:
Gmail ist kein Telekommunikationsdienst

Am 13. Juni 2019 hat der Europäische Gerichtshof (EuGH) entschieden, dass Googles Maildienst Gmail kein Telekommunikationsdienst im Sinne des EU-Rechts ist. Diese Entscheidung hat erhebliche Auswirkungen auf die Rechte und Pflichten der Anbieter sowie auf die datenschutzrechtliche Bewertung von internetbasierten E-Mail-Diensten.

Die Entscheidung des EuGH beantwortet ein Ersuchen des Oberverwaltungsgerichts (OVG) Nordrhein-Westfalen. Vorangegangen war ein Rechtsstreit zwischen der Google LLC und der Bundesrepublik Deutschland über einen Bescheid der Bundesnetzagentur (BNetzA). In dem Bescheid vom 12.7.2012 wurde erstens festgestellt, dass es sich bei dem E-Mail-Dienst Gmail von Google LLC um einen Telekommunikationsdienst handelt. Zweitens wurde Google unter Androhung eines Zwangsgelds aufgefordert, der Meldepflicht gemäß § 6 Telekommunikationsgesetz (TKG) nachzukommen. Den Widerspruch Googles gegen diesen Bescheid wies die BNetzA im Dezember 2014 als unbegründet zurück. Die beim Verwaltungsgericht Köln eingereichte Klage von Google wurde ebenfalls abgewiesen. Daher legte Google gegen die Entscheidung beim OVG Nordrhein-Westfalen Berufung ein. Dieses hat dem EuGH die Schlüsselfrage des Rechtsstreits gestellt: ob Gmail ein Telekommunikationsdienst ist.

Kernaussagen der EuGH-Entscheidung

Der EuGH stellte fest, dass Gmail kein elektronischer Kommunikationsdienst im Sinne der europäischen Datenschutzrichtlinie für elektronische Kommunikation und damit auch kein Telekommunikationsdienst im Sinne des nationalen TKG ist. Auch wenn unterschiedliche Begriffe im europäischen und im deutschen Recht verwendet werden, weisen sie die identische prägende Eigenschaft auf: Die Dienste bestehen ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze. Der E-Mail-Anbieter nehme zwar eine Übertragung von Signalen vor. Allerdings führe dies nicht

dazu, dass der Dienst überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestünde. Verantwortlich für die Übertragung der Signale seien vornehmlich die Internetanbieter (wie beispielsweise 1&1, T-Online, Kabel Deutschland), der Absender und der Empfänger von E-Mails sowie die Betreiber der verschiedenen Netze, aus denen das offene Internet besteht. Diese würden die Übertragung der Signale sicherstellen, die für internetbasierte E-Mail-Dienste erforderlich sind. Die Unterstützungstätigkeiten des E-Mail-Dienstleisters reichen nach Auffassung des EuGH nicht aus, um diesen Dienst als Telekommunikationsdienst einzustufen.

Bisher andere Auffassung der Aufsichtsbehörden

Diese Entscheidung ist zwar im Zusammenhang mit den regulierungsrechtlichen Vorschriften des TKG ergangen, sie hat aber auch auf das Datenschutzrecht erhebliche Auswirkungen. Die deutschen Aufsichtsbehörden haben bisher eine andere Rechtsauffassung vertreten und internetbasierte E-Mail-Dienste als Telekommunikationsdienste eingeordnet. Dies führte dazu, dass erstens grundsätzlich die bereichsspezifischen Datenschutzvorschriften des TKG[1] bei der Datenverarbeitung durch Telekommunikationsdienstleister zu beachten sind. Zweitens sehen Bundesdatenschutzgesetz (BDSG) und TKG[2] eine Sonderzuständigkeit des Bundesbeauftragten für Datenschutz und Informationsfreiheit für die Datenschutzaufsicht (BfDI) über Telekommunikationsdienstleister vor. Entsprechend war für die Bearbeitung von Datenschutzbeschwerden und die Beratung von TKG-Unternehmen ausschließlich der BfDI zuständig, unabhängig davon, in welchem Bundesland das TKG-Unternehmen seinen Firmensitz hat.

DSK-Beschluss: https://t1p.de/E-MailundOTT

Angesichts der EuGH-Entscheidung fasste die Datenschutzkonferenz des Bundes und der Länder (DSK) am 12. September 2019 den Beschluss „Sachliche Zuständigkeit für E-Mail und andere Over-the-top (OTT)-Dienste“. In diesem wird erstens festgestellt, dass die Datenschutzaufsicht über Webmail-Dienste den jeweils zuständigen Landesbeauftragten für den Datenschutz obliegt. Zweitens wird klargestellt, dass Messenger-Dienste, die in einem geschlossenen System operieren, wie z. B. Signal, Threema, WhatsApp, als Telekommunikationsdienste bewertet werden und die Datenschutzaufsicht weiterhin in die Sonderzuständigkeit des BfDI fällt.

1 Die §§ 91 ff. TKG

2 §§ 9 Abs. 1 BDSG und § 115 Abs. 4 TKG

Die Entscheidung des EuGH hat für meine Behörde zur Folge, dass ihr die Zuständigkeit über die Datenschutzaufsicht für E-Mail-Dienstleister mit Sitz in Niedersachsen zugefallen ist. Auch wenn in Niedersachsen nur E-Mail-Dienstleister mit einem eher geringen Marktanteil ansässig sind, muss in meinem Haus die nötige Fachkompetenz aufgebaut werden, um die datenschutzrechtliche Kontrolle und Aufklärung wahrnehmen zu können.

EuGH-Urteil von kurzer Dauer

Allerdings wird die Entscheidung des EuGH voraussichtlich nur eine kurze Wirkkraft entfalten. Denn die europäische Rahmenrichtlinie für elektronische Kommunikationsnetze und -dienste, auf der die Entscheidung beruht, ist im Dezember 2018 durch eine neue EU-Richtlinie – den europäischen Kodex für die elektronische Kommunikation – ersetzt worden. Die EU-Mitgliedstaaten sind verpflichtet, die Richtlinie bis zum 21. Dezember 2020 in nationales Recht umzusetzen. Die Definition der elektronischen Kommunikationsdienste erfasst ausdrücklich interpersonelle Kommunikationsdienste. In den Erwägungsgründen werden E-Mail-Dienste als Beispiel für elektronische Kommunikationsdienste angeführt. Es ist daher davon auszugehen, dass voraussichtlich ab 2021 die Zuständigkeit für internetbasierte E-Mail-Dienste zurück an den BfDI fällt. Der Zeitpunkt der EuGH-Entscheidung hätte aus Sicht der Aufsichtsbehörden somit kaum unglücklicher sein können, weil sich die Zuständigkeit nur für einen sehr kurzen Zeitraum verschieben wird.

Zuständigkeit geht an BfDI zurück

F. 2. Fashion-ID-Urteil:

Gemeinsame Verantwortlichkeit für Social Plugins

Bindet der Betreiber einer Webseite den „Gefällt mir"-Button von Facebook ein, dann ist er gemeinsam mit Facebook für die Erhebung und Übermittlung von Daten der Nutzer seiner Webeseite verantwortlich. Das stellte der Europäische Gerichtshof (EuGH) 2019 in einem Urteil fest.

Der EuGH-Entscheidung[1] liegt ein Rechtsstreit vor dem Landgericht Düsseldorf zwischen der Fashion ID GmbH & Co. KG und der Verbraucherzentrale NRW e. V. zugrunde. Fashion ID, ein Online-Händler für Modeartikel, hatte in seine Webseite das Facebook-Plugin „Gefällt mir" eingebunden. Die Verbraucherzentrale NRW klagte vor dem Landgericht (LG) Düsseldorf gegen Fashion ID auf Unterlassung der (automatischen) Übermittlung von personenbezogenen Daten der Webseitennutzer an Facebook Irland ohne deren Einwilligung und unter Verstoß gegen die Informationspflichten der Datenschutz-Grundverordnung (DS-GVO). Das LG Düsseldorf gab den Anträgen der Verbraucherzentrale NRW teilweise statt. Fashion ID legte gegen diese Entscheidung beim Oberlandesgericht Düsseldorf Berufung ein. Dieses legte dem EuGH mehrere Fragen zur Vorabentscheidung vor. Kernfrage des Rechtsstreits war, ob der Betreiber einer Webseite datenschutzrechtlich Verantwortlicher ist, wenn er Programmcode einbindet, der den Browser des Benutzers veranlasst, Inhalte von einem Dritten anzufordern und hierzu personenbezogene Daten an den Dritten zu übermitteln.

Datenübermittlung ohne Einwilligung

EuGH betont Verantwortung von Seitenbetreibern

Der EuGH betont mit seinem Urteil, dass jede natürliche oder juristische Person, die aus Eigeninteresse auf die Verarbeitung personenbezogener Daten Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel dieser Verarbeitung mitwirkt, für die Verarbeitung verantwortlich ist. Fashion ID habe es durch die Einbindung des „Gefällt mir"-Buttons von Facebook ermöglicht, dass beim Aufruf ihrer Webseite Nutzerdaten erhoben und an Facebook übermittelt werden. Dies geschieht unabhängig davon, ob

- der Nutzer den „Gefällt-mir" Button auf der Webseite aktiv anklickt,
- der Nutzer ein Mitglied im sozialen Netzwerk von Facebook ist und
- der Nutzer Kenntnis von dem Vorgang nimmt.

Durch diese Entscheidung wird klargestellt, dass der Betreiber einer Webseite grundsätzlich für alle Verarbeitungen personenbezogener Daten der Nutzer

1 AZ C-40/17

seiner Webseite verantwortlich ist. Und zwar auch dann, wenn sie nicht von ihm selbst durchgeführt werden. Auf nahezu jeder Webseite sind Dienste Dritter integriert wie Social Plugins, interaktive Karten, Videos, Schriften oder Cookies. All diese Dienste erfordern, dass bei der Erstellung der Webseite Programmcode des Dritten integriert wird, der in der Regel dazu führt, dass bei einem Aufruf der Webseite die Nutzerdaten nicht nur an den Server der Webseite, sondern auch an die Drittdienstleister übermittelt werden. Der EuGH stellt sich klar auf den Standpunkt, dass ohne die Einbindung des Programmcodes die Verarbeitung der Nutzerdaten durch die Drittdienstleister nicht möglich wäre. Folgerichtig trägt der Betreiber der Webseite mindestens für die Erhebung und die Übermittlung der Daten die Verantwortung.

Rechtsauffassung der Aufsichtsbehörden bestätigt

Lückenlose Zuweisung der Verantwortlichkeit möglich

Ich begrüße die Entscheidung des EuGH aus mehreren Gründen. Die Verarbeitung von Nutzerdaten im Internet ist aufgrund der Vielzahl der Akteure und der Einbindung von Drittdienstleistern auf nahezu jeder Webseite mittlerweile sehr komplex. Die Entscheidung des Gerichts zeigt auf, dass die Datenschutzvorschriften dennoch eine lückenlose und effiziente Zuweisung der datenschutzrechtlichen Verantwortung ermöglichen.

Betroffenen wäre die Wahrnehmung ihrer Rechte deutlich erschwert worden, wenn Betreiber von Webseiten nicht als Verantwortliche eingestuft worden wären. Nutzern von Webseiten ist häufig nicht einmal bekannt, dass und an wen ihre Daten beim Öffnen einer Webseite übermittelt werden, geschweige denn wie und zu welchen Zwecken sie anschließend verarbeitet werden. Die Aufsichtsbehörden werden in ihrer Rechtsauffassung zur Verwendung von Social Plugins bestätigt.

Schließlich besteht die Hoffnung, dass die Wertungen des Gerichts beim Erlass der E-Privacy-Verordnung Berücksichtigung finden werden. Social Plugins dienen nur vordergründig dem Zweck, Nutzern eine einfache Möglichkeit zu geben, interessante Inhalte im Internet in ihr soziales Netzwerk zu kommunizieren. Primär dienen sie dem Nutzertracking und der Erstellung von Persönlichkeitsprofilen, um ein individualisiertes Webmarketing zu ermöglichen. Der EuGH stellt fest, dass sowohl Betreiber der Webseite als auch Drittdienstleister mit den Social Plugins wirtschaftliche Interessen verfolgen. Entsprechend sollte jeder Betroffene frei darüber entscheiden können, ob er seine Daten dafür zur Verfügung stellen möchte oder nicht.

F. 3. Europäischer Gerichtshof überprüft Standardvertragsklauseln

Im ersten Halbjahr 2020 wird das Urteil des Europäischen Gerichtshofs (EuGH) in Sachen Schrems II erwartet. Darin wird der EuGH darüber entscheiden, ob die Übermittlung personenbezogener Daten in die USA weiterhin auf die Verwendung von Standardvertragsklauseln gestützt werden kann.

Die Verwendung von Standardvertragsklauseln[1] ermöglicht es Verantwortlichen, personenbezogene Daten in ein Drittland außerhalb der EU zu exportieren. Facebook hat für den Datenexport in die USA von dieser Möglichkeit Gebrauch gemacht. Der EuGH hat nach einer Beschwerde des österreichischen Juristen und Datenschutzaktivisten Max Schrems darüber zu entscheiden, ob und inwieweit Datenübermittlungen in die USA auf der Grundlage von Standardvertragsklauseln noch zulässig sind.

Stärkung der Rolle der Aufsichtsbehörden?

Generalanwalt: Standardvertragsklauseln weiter gültig

Im Dezember 2019 hat der Generalanwalt beim EuGH, Saugmandsgaard Øe, seinen Schlussantrag gestellt, der für das Gericht empfehlenden Charakter hat. Der Generalanwalt kommt zu dem Schluss, dass der Beschluss der Europäischen Kommission zum Erlass der Standardvertragsklauseln weiterhin gültig ist. Die Standardvertragsklauseln könnten grundsätzlich weiterverwendet werden. Datenexporte auf dieser Grundlage seien aber nur dann rechtmäßig, wenn der Schutz der Rechte der Betroffenen in der Praxis tatsächlich auch gewährleistet sei.

Nach Auffassung des Generalanwaltes hätten die Datenschutzaufsichtsbehörden die Aufsichtspflicht bei Datenübermittlungen, die auf der Verwendung von Standardvertragsklauseln beruhen. Wenn der Schutz der Rechte der Betroffenen trotz Standardvertragsklauseln nicht gewährleistet werden könne, müssten die Aufsichtsbehörden die Datenübermittlung beenden.

Dies würde die Aufsichtsbehörden in ihrer Arbeit deutlich stärken. Doch dafür wäre es zunächst notwendig, dass der EuGH dem Schlussantrag des Generalanwaltes folgt. Mit einer Entscheidung des EuGHs ist im ersten Halbjahr 2020 zu rechnen.

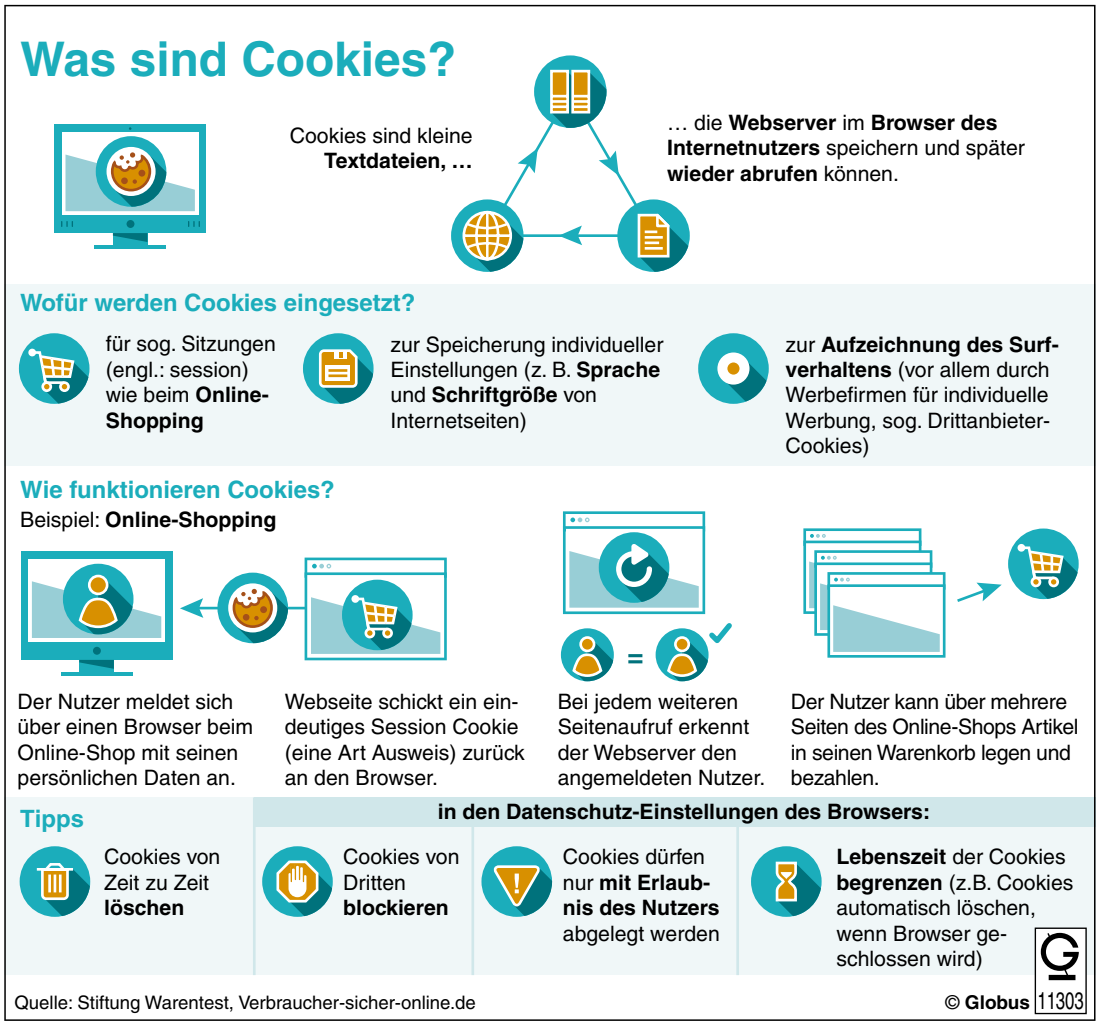
1 gem. Art. 46 Abs. 2 lit. c) DS-GVO

F. 4. Planet49-Urteil:

Zentrale Aussagen zum Tracking

Im Oktober 2019 hat der Europäische Gerichtshof (EuGH) entschieden, dass personenbezogene Daten nur dann mit Hilfe von Cookies verarbeitet werden dürfen, wenn der Nutzer aktiv einwilligt. Eine vorab eingestellte Einwilligung im Cookie-Banner ist nicht zulässig. Obwohl das Urteil die allgemeine Rechtsauffassung wiederspiegelt, sorgte es für Aufruhr.

Die EuGH-Entscheidung[1] beantwortet ein Vorabentscheidungsersuchen des Bundesgerichtshofes (BGH) im Rechtsstreit zwischen dem Verbraucherzentrale Bundesverband e. V. (VZBV) und dem Unternehmen Planet49 GmbH. Gegenstand des Verfahrens war ein Gewinnspiel auf der Webseite des Unternehmens. Nahm ein Nutzer teil, wurden unter den Eingabefeldern zwei Hinweistexte angezeigt, die mit Kästchen zum Ankreuzen versehen waren:



1 EuGH (C-673/17)

Der erste Text, dessen Kästchen nicht mit einem voreingestellten Häkchen versehen war, bezog sich auf das Einverständnis für Werbung von Sponsoren und Kooperationspartnern per Post, Telefon und E-Mail.

Durch den zweiten Hinweistext, dessen Kästchen mit einem voreingestellten Häkchen versehen war, sollte eine Einwilligung für den Einsatz eines Web-Analysedienstes erklärt werden. Durch diesen wurden Cookies gesetzt, das Surf- und Nutzungsverhalten ausgewertet sowie „interessengerechte" Werbung ermöglicht.

Häkchen für Webanalyse vorab gesetzt

Nach einer erfolglosen Abmahnung klagte der VZBV auf Unterlassung mit der Begründung, dass die Einverständniserklärungen nicht den Anforderungen des Gesetzes gegen den unlauteren Wettbewerb und des Datenschutzrechts genügten. In der ersten Instanz war die Unterlassungsklage erfolgreich, nicht aber in der Berufungsinstanz, weshalb der VZBV schließlich beim BGH in Revision ging.

Kernaussagen der EuGH-Entscheidung

Die Entscheidung ist wichtig, da zum ersten Mal Aussagen zu materiellrechtlichen Vorschriften der Datenschutz-Grundverordnung (DS-GVO) getroffen werden. Im Ergebnis hat der EuGH vier Feststellungen getroffen:

1. Eine wirksame Einwilligung gem. Art. 4 Nr. 11 und Art. 6 Abs. 1 Buchstabe a DS-GVO erfordern eine aktive Handlung des Betroffenen. Diese liegt nicht vor, wenn auf einer Webseite ein Ankreuzkästchen mit einem voreingestellten Häkchen versehen ist.
2. Werden auf einer Webseite Cookies eingesetzt, die nur mit einer Einwilligung rechtmäßig sind, ist die Einwilligung bereits für das Setzen der Cookies erforderlich.
3. In Bezug auf die Einwilligungsbedürftigkeit für den Einsatz von Cookies kommt es gemäß Art. 5 Abs. 3 Datenschutzrichtlinie für elektronische Kommunikation auf einen Personenbezug nicht an.
4. Beim Einsatz von Cookies ist der Betreiber der Webseite gemäß Art. 13 DS-GVO verpflichtet, konkrete Angaben zur Funktionsdauer der Cookies zu geben und dazu, ob Dritte Zugriff auf die Cookies erhalten können.

Aktive Handlung nötig

Die Entscheidung des EuGH enthält für mein Haus keine neuen datenschutzrechtlichen Erkenntnisse, die Rechtsauffassung der Datenschutzaufsichtsbehörden wird durch sie bestätigt. Damit werden meine Bemühungen um ein rechtskonformes Webtracking erleichtert. Die Konferenz der unabhängigen Aufsichtsbehörden (DSK) hat in der Orientierungshilfe für Anbieter von Telemedien im März 2019 umfassend die datenschutzrechtlichen Anforderungen für das Webtracking dargelegt. Die Orientierungshilfe entspricht allen vier Feststellungen des EuGH und führt sie weiter aus (siehe Kapitel E.8 auf Seite 47).

Rechtsauffassung der DSK bestätigt

Überraschend ist allerdings die Wahrnehmung der EuGH-Entscheidung in der Praxis. In zahlreichen Berichten wird aus ihr – teilweise mit Empörung und Entsetzen verbunden – die Kernaussagen des EuGH, „keine Cookies ohne Einwilligung" gezogen. Diese Feststellung findet sich allerdings nicht in der Entscheidung, da keine diesbezügliche Vorlagefrage gestellt worden war. Eine Antwort auf die für die Praxis bedeutsame Frage, ob der Einsatz von Cookies grundsätzlich nur mit einer Einwilligung rechtmäßig erfolgt, gibt aber besagte Orientierungshilfe. In dieser wird differenziert dargestellt, dass für den rechtmäßigen Einsatz von Cookies grundsätzlich eine Einwilligung, ein Vertrag oder ein berechtigtes Interesse bei nicht überwiegenden Betroffeneninteressen in Betracht kommen (Art. 6 Abs. 1 Buchstabe a, b oder f DS-GVO).

Orientierungshilfe für Anbieter von Telemedien: https://t1p.de/OHTracking

F. 5. Entscheidung des Bundesverwaltungsgerichts:

Welches Recht gilt für Altfälle?

Datenschutzverstöße, die nach dem Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 begangen wurden, werden nach den gesetzlichen Vorgaben der Verordnung bewertet. Welches Recht gilt aber für die sogenannten Altfälle?

Bei einer Änderung der Gesetzeslage – wie sie mit dem Geltungsbeginn der DS-GVO eingetreten ist – ist zu klären, welches Recht auf Verfahren angewendet wird, die vor der Gesetzesänderung von der Aufsichtsbehörde abgeschlossen, aber noch nicht durch ein Gericht geprüft worden sind. Diese Frage stellt sich auch in den Fällen, in denen ein Fehlverhalten zwar vor der Gesetzesänderung beendet wurde, aber die Behörde die Aufsichtsmaßnahme erst danach trifft.

Keine Übergangsregelung für die DS-GVO

Um solche Regelungslücken zu vermeiden, sollte der Gesetzgeber für Altfälle Übergangsvorschriften festlegen. Für die DS-GVO gibt es solche Regelungen jedoch nicht.

Fallgruppe 1: Entscheidung des Bundesverwaltungsgerichts

Das Bundesverwaltungsgericht (BVerwG) hat sich in einer Revisionsentscheidung[1] zu den Grenzen der Videoüberwachung in einer Zahnarztpraxis zur ersten der oben genannten Fallgestaltungen eindeutig positioniert: Demnach findet die DS-GVO keine Anwendung auf datenschutzrechtliche Anordnungen, die vor diesem Zeitpunkt erlassen worden sind. Diese Entscheidungen werden nicht nachträglich an den Vorgaben der neuen Verordnung gemessen. Stattdessen ist auf sie die zum Zeitpunkt der Behördenentscheidung geltende nationale Rechtslage anzuwenden.

Das BVerwG begründete seine Entscheidung damit, dass behördliche Ermessensentscheidungen nur eingeschränkt gerichtlich überprüfbar seien. Dies schließe grundsätzlich aus, Ermessensentscheidungen anhand von tatsächlichen und rechtlichen Erkenntnissen nachzuprüfen, die die Behörde nicht in ihre Erwägungen einbeziehen konnte, weil sie zum Zeitpunkt der Entscheidung noch nicht vorlagen.

Ich begrüße diese Entscheidung, denn es wäre nicht sachgerecht, die Rechtmäßigkeit der Ermessensentscheidungen meiner Behörde grundsätzlich anhand einer mir nicht erkennbaren Sach- oder Rechtslage nachträglich zu bewerten.

Im Übrigen wird meine Behörde natürlich eine nach meiner Entscheidung eingetretene Rechts- oder Tatsachenänderung berücksichtigen, sofern diese im Lauf eines verwaltungsgerichtlichen Verfahrens eintritt bzw. vorgebracht wird. Bei diesen Sachlagen ist in jedem Einzelfall die Möglichkeit eines Widerrufs meiner Behördenentscheidung für die Zukunft möglich. Die Rechtmäßigkeit meiner ursprünglichen Entscheidung wird davon jedoch nicht betroffen.

Nebenentscheidung zur Videoüberwachung durch private Stellen

Darüber hinaus hat das BVerwG festgestellt, dass sich eine Videoüberwachung öffentlich zugänglicher Räume durch private Verantwortliche nicht auf den zeitgleich zum Wirksamwerden der DS-GVO in Kraft getretenen § 4 Absatz 1 Satz 1 BDSG n. F. stützen könne. Es bliebe kein Raum für eine Anwendung der Norm. In der DS-GVO seien keine Öffnungsklauseln für den nationalen Gesetzgeber für den Erlass des § 4 BDSG n. F. für private Stellen vorgesehen.

Keine Öffnungsklausel für § 4 BDSG n.F.

Diese Rechtsansicht entspricht auch meiner Auffassung. Danach ist § 4 BDSG n. F. in Bezug auf private Stellen als nicht europarechtskonform einzustufen. Für die Bewertung, ob eine Videoüberwachung in öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen rechtmäßig ist, kommt als Rechtsgrundlage allein Artikel 6 Absatz 1 lit. f DS-GVO als abschließende Regelung in Betracht (berechtigtes Interesse).

Dementsprechend hat meine Behörde bereits mit Geltungsbeginn der DS-GVO die durch private Stellen betriebenen Videoüberwachungsanlagen allein anhand dieser Norm auf ihre Rechtmäßigkeit geprüft. Um unverhältnismäßigen Änderungsaufwand zu vermeiden, habe ich es bisher

FAQ zur Videoüberwachung: https://t1p.de/faq-video

1 1 BVerwG, Az 6 C 2.18, Urteil vom 27. März 2019

nicht beanstandet, wenn auf der Hinweisbeschilderung als Rechtsgrundlage der Verarbeitung neben Artikel 6 Absatz 1 lit. f DS-GVO auch § 4 BDSG n. F. genannt wurde. Allerdings sind die zur Erfüllung der Informationspflichten nach Artikel 13 Absatz 1 lit. c DS-GVO verwendeten Hinweise entsprechend der Rechtsprechung des BVerwG anzupassen.

Fallgruppe 2: Verwaltungsverfahren der LfD

Meine Behörde erhielt die Beschwerde eines Beschäftigten über eine GPS-Überwachung eines privaten Pkws durch den Arbeitgeber. Die Überwachung wurde bereits vor Geltung der DS-GVO beendet. Die aufsichtsrechtliche Verfügung erging jedoch erst nach dem 25. Mai 2018. Gegen diese Verfügung wurde vor dem Verwaltungsgericht Klage erhoben.

Im Verfahren habe ich verdeutlicht, dass im Hinblick auf die Bewertung des Fehlverhaltens der Arbeitgeberin allein auf die Rechtslage gemäß § 32 BDSG alter Fassung (a. F.) abzustellen ist. Als die rechtswidrige Überwachung des Beschäftigten beendet wurde, war § 26 BDSG n. F. noch nicht in Kraft. Ob ein Verhalten rechtswidrig ist, kann jedoch nur anhand einer zur gleichen Zeit geltenden Rechtsnorm bewertet werden.

Allerdings konnte ich für meine Verfügung nicht mehr auf § 38 Absatz 5 BDSG a. F. zurückgreifen. Diese Ermächtigungsgrundlage war zum Zeitpunkt der behördlichen Entscheidung außer Kraft. Ich konnte mich auch nicht unmittelbar auf die Abhilfebefugnis einer Verwarnung nach Artikel 58 Absatz 2 lit. b DS-GVO stützen. Der Wortlaut der Norm sieht ausdrücklich den Anwendungsbereich nur für Verstöße „gegen diese Verordnung" vor. Es liegt – mangels Übergangsvorschrift – eine Regelungslücke vor, die mit einer Analogie geschlossen werden kann.

Regelungslücke mit Analogie schließen

Die Regelungslücke ist planwidrig. Aus den Erwägungsgründen zur DS-GVO sowie den Gesetzesbegründungen zum BDSG und NDSG ist nicht erkennbar, dass der Gesetzgeber die Lücke bewusst herbeigeführt hat. Darüber hinaus liefe die Annahme einer bewussten Gesetzeslücke dem von DS-GVO und BDSG n. F. bezweckten verbesserten Schutz personenbezogener Daten zuwider. Der Gesetzgeber hatte bis zum 25. Mai 2018 mit § 38 Absatz 5 BDSG a. F. eine Befugnisnorm für die Ahndung von Verstößen gegen datenschutzrechtliche Bestimmungen für die Aufsichtsbehörden vorgesehen. Es würde dem Schutzziel widersprechen, wenn er plötzlich keine Ermächtigungsnorm mehr für beendete rechtswidrige Handlungen vorsehen wollte.

Auch ist die Interessenlage vergleichbar. Es muss mir als Aufsichtsbehörde gestattet sein, Abhilfemaßnahmen nach Artikel 58 Absatz 2 DS-GVO auch für vor dem Inkrafttreten der DS-GVO erledigte Verstöße zu ergreifen. Augenfällig wird dies besonders in den Fällen, in denen sich die Verstöße gegen materielle Regelungen des BDSG a. F. auch nach neuer Rechtslage als rechtswidrig erweisen würden. Deutlich wird das anhand der – im vorliegenden Fall einschlägigen – nahezu identischen Regelungen einerseits in § 32 BDSG a. F. sowie andererseits in Artikel 6 Absatz 2 und Absatz 3 in Verbindung mit Artikel 88 DS-GVO in Verbindung mit § 26 BDSG n. F. Die beiden Gesetze erlauben bzw. erlaubten die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis nur in engen Grenzen. Es wäre unbillig, wenn derartige Fälle nur deshalb keiner aufsichtsrechtlichen Maßnahme unterzogen werden könnten, weil sie beispielsweise erst nach dem 25. Mai 2018 oder kurz zuvor bekannt wurden und deshalb nicht mehr abschließend von der Aufsichtsbehörde bearbeitet werden konnten.

Fast identische Regelungen in altem und neuem Recht

Ob die von mir vertretene Rechtsauffassung in diesem konkreten Fall vom Verwaltungsgericht geteilt wird, stand bei Redaktionsschluss noch nicht fest.

G. Beteiligung an Gesetzgebungsverfahren

G.1. Neues Polizeigesetz weiter verbesserungsbedürftig

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

In meinem Tätigkeitsbericht 2017-2018 habe ich bereits über die hitzige Diskussion zum Entwurf des neuen Polizeigesetzes (NPOG) berichtet. Zum Redaktionsschluss des damaligen Berichts war das parlamentarische Verfahren noch nicht abgeschlossen. Zudem hat das NPOG mit dem „Gesetz zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes" vom 17. Dezember 2019 eine weitere wesentliche Änderung erfahren. Deshalb greife ich das Thema nun erneut auf.

Der Landtag hatte mir im Rahmen einer öffentlichen Anhörung am 9. August 2018 die Möglichkeit zur Stellungnahme gegeben. Der Entwurf konnte im weiteren Gesetzgebungsverfahren an vielen Stellen aus Sicht des Datenschutzes verbessert werden. Dennoch blieben zahlreiche Kritikpunkte bestehen.

Staatstrojaner verfassungsrechtlich fragwürdig

Besonders kritisch beurteile ich die neu geschaffenen Maßnahmen der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) nach § 33a Abs. 2 NPOG und der Online-Durchsuchung (§ 33d NPOG). Diese Instrumente erlauben der Polizei einen tiefen Einblick in die Privatsphäre der Betroffenen.

Bürger müssen vor Cyberangriffen geschützt werden

In beiden Fällen installieren die Sicherheitsbehörden ohne Kenntnis der Betroffenen eine Software auf deren Endgerät (Smartphone oder Computer). Dafür müssen sie Sicherheitslücken in der Betriebssoftware nutzen, von denen auch Kriminelle profitieren können. Dieses Verhalten steht im Widerspruch zur staatlichen Pflicht, die Bürgerinnen und Bürger unverzüglich über Sicherheitslücken im Internet aufzuklären, um so einen umfassenden Schutz vor Cyberangriffen zu gewährleisten. Will die Polizei die Quellen-TKÜ oder Online-Durchsuchung einsetzen, so muss sie bekannte Sicherheitslücken bewusst offenhalten (und damit verschweigen) oder im schlimmsten Fall sogar Dienstleistungen von Hackern ankaufen.

Problematisch ist zudem, dass die Polizei mit Hilfe des Staatstrojaners grundsätzlich auf alle Daten des Betroffenen zugreifen kann. Dies wäre jedoch unverhältnismäßig und damit verfassungswidrig. Die Software muss daher auf einen bestimmten Anwendungsbereich reduziert werden, sodass sie z. B. nicht auf Daten zugreifen kann, die in den Kernbereich privater Lebensgestaltung fallen. Das Gesetz macht zwar Vorgaben hierzu. Ob diese allerdings tatsächlich umsetzbar sind, um einen missbräuchlichen Einsatz zu verhindern, ist verfassungsrechtlich noch ungeklärt.

Unbeantwortet ist bislang auch die Frage, ob die Quellen-TKÜ und die Online-Durchsuchung tatsächlich für die Polizei erforderlich sind, um Straftaten zu verhindern und, ob diese Instrumente mit Augenmaß eingesetzt werden. Der Gesetzgeber hat festgelegt, dass die neuen Befugnisse Ende 2024 überprüft werden sollen.

Unverhältnismäßige Videoüberwachung

Verdeckte Überwachung weiter erlaubt

Inakzeptabel sind auch zahlreiche Regelungen, die sich mit der Videoüberwachung befassen. So wird die Videoüberwachung im öffentlichen Raum massiv verstärkt, weil nun Bildaufzeichnungen zulässig sind, wenn an einem bestimmten Ort Straftaten – auch geringfügige – begangen werden. Nach altem Recht durften Bildaufzeichnungen nur dann angefertigt werden, wenn „schwere" Straftaten zu erwarten waren.

Das neue Gesetz erlaubt weiterhin die verdeckte und damit für den Bürger unbemerkte Videoüberwachung von öffentlichen Orten, an denen wiederholt Verbrechen begangen wurden. Dies halte ich für verfassungswidrig, da eine verdeckte Maßnahme keine präventive Wirkung entfalten kann und nur dem Zweck der Strafverfolgung dient. Hierfür fehlt dem Landesgesetzgeber aber die Gesetzgebungskompetenz.

Gleiches gilt für die Videoüberwachung mit der sogenannten Pre-Recording-Funktion von Bodycams. Auch dort werden für den Betroffenen oftmals unbemerkt Bildaufzeichnungen angefertigt. Diese werden zwar fortlaufend nach einer kurzen Speicherzeit überschrieben. Dennoch findet unbestreitbar eine Datenverarbeitung statt, der insbesondere im Fall eines Strafverfahrens eine Beweisfunktion zukommt. Auch hier dürfte die Gesetzgebungskompetenz

des Landes fraglich sein. Hinzu kommt, dass die verdeckte permanente Datenspeicherung an keine Voraussetzungen geknüpft und damit anlasslos ist. Dies ist verfassungsrechtlich ebenfalls nicht zu rechtfertigen.

JI-Richtlinie nicht umgesetzt

Der Gesetzgeber hat mit dem Reformgesetz wissentlich und willentlich die „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung" (sogenannte JI-Richtlinie)[1] nicht umgesetzt. Ein aus meiner Sicht nicht hinnehmbarer Zustand, denn die Frist hierfür ist am 6. Mai 2018 abgelaufen. Damit sind wesentliche Teile des Gefahrenabwehrrechts, die sich mit der polizeilichen Datenverarbeitung beschäftigen, europarechtswidrig. Dieser Zustand muss schnellstmöglich beendet werden.

Forderungen der LfD umgesetzt

Im Datenschutzrecht gilt der Grundsatz, dass in das Recht auf informationelle Selbstbestimmung nur eingegriffen werden darf, wenn der Gesetzgeber zuvor klare und bestimmte Regelungen hierfür getroffen hat. Das Reformgesetz setzte erfreulicherweise Weise an einigen Stellen diese grundlegende Forderung meiner Behörde um, die ich schon seit geraumer Zeit für vier Maßnahmen erhoben habe.

Grundlagen für Bodycams und Section Control

So regelt der Gesetzgeber ausdrücklich in § 32 Abs. 4 NPOG, unter welchen Voraussetzungen die Polizei – unbeschadet des kritisierten Pre-Recordings – Bodycams einsetzen darf und zu welchen Zwecken die erhobenen Daten verarbeitet werden dürfen. Auch wurden in § 32 Abs. 6 NPOG gesetzliche Regelungen für die Abschnittskontrolle zur Geschwindigkeitsüberwachung (Section Control) sowie in § 32 Abs. 5 NPOG zur Videoüberwachung zur Lenkung des Straßenverkehrs geschaffen. Die Bildüberwachung von Personen, die sich im Polizeigewahrsam befinden, ist ebenfalls nun ausdrücklich im NPOG festgeschrieben.

Verbesserungen des Reformgesetzes

Im Rahmen der Anhörung hatte ich eine Reihe von Vorschlägen zur Verbesserung des Datenschutzes unterbreitet. Zwar wurden nicht alle berücksichtigt, doch es ist mir gelungen, das Datenschutzniveau an einigen Stellen wesentlich anzuheben. So können die Maßnahmen der elektronischen Aufenthaltsüberwachung, Kontaktverbote, Aufenthaltsvorgaben oder längerfristige Meldeauflagen nur nach vorheriger Anordnung durch einen Richter durchgeführt werden. Der Gesetzentwurf sah hier ursprünglich noch eine polizeiliche Anordnung vor. Erstmals sieht das NPOG zudem Höchstspeicherfristen für die Videoüberwachung vor, wie es in anderen Ländern bereits üblich war (§ 32 Abs. 3 Satz 5 und § 32 Abs. 4 Satz 5 ff NPOG). So darf Bildmaterial im Regelfall nur für einen Zeitraum von sechs Wochen gespeichert werden. Die Behörden sind gezwungen, die Bildaufzeichnungen zügig auszuwerten, so dass eine Speicherung auf Vorrat vermieden wird.

Besonders erfreulich ist es, dass nun im Polizeirecht nahezu durchgängig Verfahrensvorschriften zur Anordnung und Durchführung der Maßnahmen verankert sind. So wird eine wirksame Kontrolle der polizeilichen Datenverarbeitung durch meine Behörde möglich. Ins-

1 https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1563364005736&uri=CELEX:32016L0680

besondere, wenn die betroffenen Bürgerinnen und Bürger keine Kenntnis von einer gegen sie gerichteten Maßnahme erhalten. So müssen verdeckt durchgeführte Überwachungsmaßnahmen wie z. B. die TKÜ oder die Wohnraumüberwachung besonders begründet und dokumentiert werden. Auch die Kontrollmöglichkeiten des Parlaments gegenüber der Polizei bei besonders grundrechtintensiven Eingriffen wurden auf meine Anregung hin gestärkt.

Wirksamere Kontrolle möglich

Änderung des NPOG

Kurz nach Inkrafttreten am 24. Mai 2019 musste das NPOG mit dem „Gesetz zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes" vom 17. Dezember 2019 bereits nachgebessert werden. Betroffen waren die Regelungen im Bereich der verdachts- und ereignisunabhängigen Kontrollen sowie Einsätze von automatisierten Kennzeichenlesesystemen.

Die Änderungen waren wegen der Beschlüsse des Bundesverfassungsgerichts (BVerfG) vom 18. Dezember 2018[2] erforderlich, in denen Teilbereiche einiger Landesgesetze zum Einsatz von automatisierten Kennzeichenlesesysteme für verfassungswidrig erklärt worden waren.

Vorgaben des Bundesverfassungsgerichts überdehnt

Ende 2019 erhielt ich die Möglichkeit, zu den beabsichtigten Gesetzesänderungen Stellung zu nehmen. Auf Grundlage der Beschlüsse des BVerfG bewertete ich die verdachtsunabhängigen Befragungen und Einsätze von automatischen Kennzeichenlesesystemen als grundsätzlich zulässig. Allerdings nur ausnahmsweise als Ausgleich zum Wegfall der Grenzkontrollen im „Schengen-Raum". Ein solcher Grenzbezug ist mit dem vorgesehenen Einsatz auch auf Bundesstraßen in einem Flächenland wie Niedersachsen nicht mehr gegeben. Entsprechend beschränkt das BVerfG die Zulässigkeit eines Einsatzes automatisierter Kennzeichenlesesysteme auf Bundesautobahnen und Europastraßen. Ob die im weiteren Gesetzgebungsverfahren eingeführte sachliche Begrenzung auf „Straftaten mit Grenzbezug" in ausreichendem Maße den verfassungsrechtlich verankerten Grundsatz der Verhältnismäßigkeit berücksichtigt, ist fraglich.

Missbrauch von Systemen zur Kennzeichenerfassung

Zum Einsatz automatisierter Kennzeichenerfassungssysteme fiel im Berichtszeitraum auf, dass in anderen Bundesländern bei der Nutzung dieser Systeme für die Strafverfolgung die Daten der Verkehrsteilnehmer massenhaft über einen längeren Zeitraum hinweg unterschiedslos erfasst und langfristig gespeichert werden. Dies ist missbräuchlich, da der angewandte § 100h Abs. 1 Satz 1 Nr. 2 der Strafprozessordnung keine ausreichende Rechtsgrundlage darstellt. Auch die Datenschutzkonferenz hat sich mit einer Entschließung ausdrücklich gegen diese rechtswidrige Verarbeitung personenbezogener Daten gewandt.

Entschließung der DSK: https://t1p.de/Kennzeichenerfassung

2 Az 1 BvR 142/15, 1 BvR 2795/09 und 1 BvR 3187/10

G.2. Digitale Verwaltung datenschutzkonform und sicher gestalten

Mit dem „Niedersächsischen Gesetz über digitale Verwaltung und Informationssicherheit“ (NDIG) soll die Einführung der digitalen Verwaltung geregelt und die IT-Sicherheit im Landesdatennetz erhöht werden. Damit wurde eine notwendige Rechtsgrundlage für den von der Landesverwaltung geplanten Einsatz von „Next Generation Firewalls“ geschaffen.

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

Bereits in meinem Tätigkeitsbericht 2017/2018 habe ich über das Gesetzgebungsverfahren zum „Gesetz zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes“ berichtet. Das Gesetz war längst überfällig und enthielt bereits im Entwurf wichtige Regelungen, z. B. zum elektronischen Zugang zur Verwaltung, zu elektronischen Bezahlmöglichkeiten und zur Einführung der elektronischen Aktenführung.

Grundsätzlich waren die Ziele des Gesetzgebungsvorhabens durchaus begrüßenswert. In meiner Stellungnahme zum Gesetzentwurf sprach ich mich dafür aus, die Regelungen zum E-Government möglichst datenschutzfreundlich zu gestalten. Die IT-Sicherheit, die durch das Gesetz für das Landesnetz geregelt werden soll, ist auch im Datenschutz ein wichtiger Faktor. Denn unzureichende IT-Sicherheitsmaßnahmen können den Schutz personenbezogener Daten gefährden. Dabei müssen die getroffenen Maßnahmen verhältnismäßig sein, also geeignet, erforderlich und angemessen. Es gilt, einen möglichst grundrechtsschonenden Ansatz zu wählen, der Zweck und Mittel in ein ausgewogenes Verhältnis bringt.

Tiefer Eingriff in Privatsphäre möglich

Wird die Auswertung von Inhaltsdaten im Datenverkehr angeordnet, so kann es sich um Datenströme etwa aus dem E-Mail-Verkehr handeln oder auch um Daten aus Telefonaten. Damit ist ein weitreichender Eingriff in personenbezogene Daten und die Privatsphäre möglich. Aus diesem Grund habe ich gefordert, die Anordnung der Auswertung von Inhaltsdaten unter Richtervorbehalt zu stellen.

Leider wurde das Gesetz am 23. Oktober 2019 ohne einen meiner Änderungsvorschläge verabschiedet. Von den Eingriffsbefugnissen darf jedoch nach § 25 Abs. 3 NDIG nur dann Gebrauch gemacht werden, wenn ein Sicherheitskonzept für die zur Auswertung genutzten technischen Systeme erstellt wurde. Zudem verbietet §19 Abs. 3 NDIG die Inhaltsdaten im Hinblick auf ihre kommunikative Bedeutung auszuwerten.

Vorschläge der LfD nicht berücksichtigt

Nach § 28 NDIG ist mir einmal jährlich eine Dokumentation vorzulegen, aus der hervorgeht, wie von den Befugnissen Gebrauch gemacht wurde. Ich werde daher prüfen, ob die vorhandenen gesetzlichen Schutzmechanismen auch in der Praxis umgesetzt werden.

G.3. Novellierung des Niedersächsischen Justizvollzugsgesetzes

Der Gesetzentwurf der Landesregierung zur Novellierung des Niedersächsischen Justizvollzugsgesetzes (NJVollzG) befindet sich derzeit im parlamentarischen Verfahren. Meine Behörde hat hierzu zuletzt schriftlich gegenüber dem zuständigen Unterausschuss des Landtages Stellung bezogen.

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

Wie bereits im Tätigkeitsbericht 2017/2018 berichtet, ist die Gesetzesänderung unter anderem durch die europäische Datenschutzreform notwendig geworden.[1] So müssen die Vorgaben der Richtlinie (EU) 2016/680 (JI-Richtlinie) in den datenschutzrechtlichen Bestimmungen des NJVollzG umgesetzt werden. Die Zusammenarbeit mit dem Justizministerium war bereits im Rahmen der Ressortabstimmung im Sommer 2018 sehr konstruktiv.

Verbandsbeteiligung und Anhörung im Ausschuss

Nachdem ich Anfang 2019 im Rahmen der Verbandsbeteiligung die Möglichkeit zur Stellungnahme genutzt hatte, erschien im Herbst 2019 mit der Drucksache 18/3764 der aktualisierte Gesetzentwurf der Landesregierung. Zu diesem war meine Behörde vom Unterausschuss „Justizvollzug und Straffälligenhilfe" des Ausschusses für Rechts- und Verfassungsfragen zur schriftlichen Anhörung aufgefordert. Der Entwurf griff bereits an verschiedenen Stellen die Kritikpunkte und Anregungen auf, die ich in der Verbandsbeteiligung vorgetragen hatte.

Aus meiner Sicht sind Nachbesserungen lediglich zu einzelnen Punkten notwendig. Dies betrifft etwa das Auslesen von Datenspeichern ohne Kenntnis der betroffenen Person. Für die praktische Anwendung sollte diese Regelung noch konkreter gefasst werden.

Ausdrücklich zu begrüßen ist die Anpassung, mit der das „Zusammenspiel" zwischen dem NJVollzG und dem Niedersächsischen Datenschutzgesetz (NDSG) geregelt wird. Hiermit werden die Vorschriften des Zweiten und Dritten Teils des NDSG für anwendbar erklärt, wenn das NJVollzG keine besonderen Regelungen enthält und Zweck und Eigenart des Vollzuges der in diesem Gesetz genannten freiheitsentziehenden Maßnahmen nicht entgegenstehen. Hierdurch wird insgesamt ein hohes Datenschutzniveau erreicht. Zugleich werden mögliche Regelungslücken vermieden.

Allerdings ist mir eine endgültige Bewertung des Gesetzesvorhabens noch nicht möglich. Bis zum Ende des Berichtszeitraums war das parlamentarische Verfahren noch nicht abgeschlossen.

1 Siehe Tätigkeitsbericht 2017-2018 unter F. 2.4, S. 64f.

G.4. Verfassungsschutzgesetz:

Konstruktive Zusammenarbeit mit dem Innenministerium

Ende September 2019 habe ich einen ersten Referentenentwurf zur Novelle des Niedersächsischen Verfassungsschutzgesetzes mit der Möglichkeit zur Stellungnahme erhalten. Bei der Auswertung des Entwurfes musste ich feststellen, dass Datenschutzregelungen nicht ausreichend berücksichtigt waren. Aus diesem Grund habe ich Anfang November 2019 eine umfassende Stellungnahme an das Niedersächsische Ministerium für Inneres und Sport übersandt.

Besonders kritisch beurteilte ich die eingeschränkten Befugnisse und Zuständigkeiten der G10-Kommission. So soll der Zustimmungsvorbehalt der G10-Kommission zum Einsatz von Vertrauenspersonen, sogenannten V-Leuten, entfallen. Weitere gewichtige Kritikpunkte sind die unzureichende Regelung meiner Kontrollbefugnisse sowie die stark eingeschränkte Anwendbarkeit des Niedersächsischen Datenschutzgesetzes (NDSG). Gerade der letzte Punkt schloss die Anwendung vieler wesentlicher datenschutzrechtlicher Vorgaben aus. Der erste Entwurf wäre damit geeignet gewesen, einen weitgehend kontrollfreien Rechtsrahmen für den Verfassungsschutz zu schaffen.

Deutliche Kritik am ersten Entwurf

Verfassungsschutz sucht Gespräch mit LfD

Als Reaktion auf meine Stellungnahme suchte der Verfassungsschutz das Gespräch mit mir und überarbeitete den Referentenentwurf des Gesetzes an mehreren Stellen im Sinne des Datenschutzes. So wurde unter anderem die nicht eindeutige Regelung zum besonderen Auskunftsverlangen umformuliert. Auch die vorher gestrichene Unterrichtungspflicht des Ausschusses für Angelegenheiten des Verfassungsschutzes wurde wieder aufgenommen.

Pflicht zur Unterrichtung wieder aufgenommen

Allerdings wurden nicht alle meine Kritikpunkte berücksichtigt. Zwar wurde die Gesetzesbegründung bei der Erhebung personenbezogener Daten bei Minderjährigen angepasst. Trotz dieser Klarstellung halte ich weiterhin an der Kritik fest, die Erhebung durch Verschieben der Altersgrenzen für Minderjährige (von 16 auf 14 Jahre beziehungsweise von 18 auf 16 Jahre) zu vereinfachen. Es wird damit dem Gesetzgeber obliegen, die besonders schutzwürdigen Interessen von Minderjährigen mit den Sicherheitsinteressen des Landes in Einklang zu bringen.

Darüber hinaus habe ich dem Verfassungsschutz weitere Empfehlungen unterbreitet, mit dem ein hohes Datenschutzniveau erreicht werden kann und gleichzeitig die Sicherheitsinteressen des Landes gewahrt werden.
Die daraufhin erneut überarbeitete Version des Entwurfes setzte mehrere Änderungen auf Grundlage meiner Stellungnahme um.

Weiteres Potenzial zur Überarbeitung

Trotz der vorgenommenen Änderungen müssen noch einige Punkte überarbeitet werden. So sollen entscheidende Regelungen aus dem NDSG keine Anwendung für den Niedersächsischen Verfassungsschutz finden:

Datenschutz-Folgenabschätzung

- Die Datenschutz-Folgenabschätzung (DSFA) nach § 39 NDSG, obwohl diese zunächst als ein Instrument der Selbstkontrolle anzusehen ist. Mit der DSFA wird dem Verantwortlichen die Möglichkeit gegeben, vorab eine Abschätzung der Folgen der Verarbeitung für den Schutz personenbezogener Daten durchzuführen, um rechtzeitig mit ausreichenden technisch-organisatorischen Schutzmaßnahmen reagieren zu können.

- Die vorherige Anhörung der Aufsichtsbehörde nach § 40 NDSG.

  Meine Behörde verfügt über ein breitgefächertes Know-how, unter anderem zu technischen und organisatorischen Maßnahmen. Im Rahmen einer Anhörung vor der Inbetriebnahme neuer Datenverarbeitungssysteme kann ich dem Verantwortlichen schriftliche Empfehlungen unterbreiten. Damit ist die verantwortliche Stelle aus behördlicher Sicht abgesichert.

Meldung von Datenpannen

- Die Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde (Datenpanne) nach § 41 NDSG. Die Datenpannenmeldung dient zunächst der Minimierung der negativen Auswirkungen von Datenschutzverletzungen, indem ich Hinweise gebe, wie der Verantwortliche mit der aktuellen Verletzung umzugehen hat, und wie er künftig Verstöße vermeiden kann.

- Die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen nach § 42 NDSG. Die Benachrichtigung dient der Risikoabwehr und der Schadensminimierung beim Betroffenen und sollte zum unmittelbaren Schutz der Rechte und Freiheiten des Betroffenen Anwendung finden. Bei einer rechtzeitigen Information des Betroffenen können etwaige Haftungsansprüche eingedämmt werden.

Vertrauliche Meldung von Verstößen

- Die vertrauliche Meldung von Verstößen nach § 43 NDSG. Die Vorschrift soll eine diskrete Behandlung von Datenpannenmeldungen garantieren. Sie dient dem Schutz von (internen und externen) Informanten, die Kenntnis von einer Datenpanne erhalten haben. Ohne Kenntnisnahme von Datenpannen hat der Verantwortliche keine Möglichkeit diese zukünftig zu unterbinden oder die Auswirkungen der derzeitigen Panne zu minimieren.

- Die allgemeinen Informationen nach § 50 NDSG. Betroffene Personen sollen unabhängig von einer konkreten Datenverarbeitung einen Überblick über die Zwecke der Verarbeitungen und eine Übersicht über die Betroffenenrechte erhalten. Das kann im Sinne einer allgemeinen Bürgerinformation auf der Webseite des Verantwortlichen geschehen. Hiermit können unter anderem Fragen der Betroffenen frühzeitig geklärt werden.

Frühe Einbindung der LfD zahlt sich aus

Bereits der Erst-Entwurf der Novelle enthielt gegenüber dem bestehenden Gesetz aber auch einige Änderungen, die datenschutzrechtlich zu begrüßen waren. So wurden begriffliche Anpassungen innerhalb des Gesetzes an das Niedersächsische Datenschutzgesetz (NDSG) vorgenommen. Weiter wurde eine spezielle Rechtsgrundlage für die Datenübermittlung an Trägereinrichtungen der Ausstiegsarbeit im rechtsradikalen Milieu.

Den offenen und konstruktiven Umgang des Niedersächsischen Verfassungsschutzes mit dem Entwurf und meine Einbindung begrüße ich außerordentlich. Es hat sich als überaus sinnvoll erwiesen, bereits in einer frühen Phase einer gesetzlichen Änderung beteiligt zu werden, um den datenschutzrechtlichen Erfordernissen Genüge zu tun. Vorbehalte, die auf beiden Seiten bestehen, lassen sich in einem Gespräch oftmals beseitigen und dürften als Ergebnis zu einem tragfähigen Entwurf führen, der im weiteren Gesetzgebungsverfahren weniger Kritik erfährt.

Ich stehe weiterhin in Kontakt mit dem Verfassungsschutz, um die aus meiner Sicht noch strittigen Punkte in dem Entwurf nochmals zu verdeutlichen.

G.5. Änderung des Niedersächsischen Schulgesetzes

Durch die Datenschutz-Grundverordnung mussten die datenschutzrechtlichen Regelungen für den Schulbereich angepasst werden. Die von mir eingebrachten Änderungsanregungen wurden im parlamentarischen Verfahren umgesetzt.

Der Niedersächsische Landtag hat erneut das Niedersächsische Schulgesetz novelliert. Neben den landesrechtlichen Anpassungen an das Pflegeberufegesetz des Bundes und Änderungen im Privatschulrecht wurden die datenschutzrechtlichen Grundlagen für den Schulbereich ergänzt (§ 31 NSchulG). Anpassungsbedarf bestand im Hinblick auf die Verarbeitung besonderer Datenkategorien. Diese Lücke, die insbesondere die Verarbeitung von Gesundheitsdaten betraf, wurde geschlossen. Zudem wurden in der Praxis erforderliche Übermittlungsbefugnisse an bestimmte öffentliche und nicht-öffentliche Stellen aufgenommen.

Befugnis für digitale Lehrmittel

Für den Einsatz digitaler Lehr- und Lernmittel sowie internetbasierter Plattformen wurde eine datenschutzrechtliche Verarbeitungsbefugnis geschaffen. Mit Inkrafttreten des Gesetzes ist nun keine schriftliche Einwilligung der Schülerinnen und Schüler bzw. ihrer Erziehungsberechtigten mehr notwendig, um im schulischen Alltag internetbasierte Angebote vorzuhalten.

Rechtssichere und übersichtliche Norm

Die im Gesetzentwurf vorgesehenen Rechtsänderungen waren so umfangreich, dass die Norm für den juristischen Laien nur noch schwer zu verstehen gewesen wäre. Zudem war die Regelung zur Verarbeitung besonderer Datenkategorien unkonkret und damit nicht DS-GVO-konform. Meine Einwände wurden im Verlauf der parlamentarischen Beratung aufgegriffen:

- Die bereits im geltenden Recht bestehenden weiten Ermächtigungen wurden konkretisiert und fallgruppenspezifisch in einzelnen Absätzen zusammengefasst,
- Die Verarbeitung besonderer Datenkategorien wurde in einem gesonderten Absatz geregelt und auf bestimmte Datenarten und Verarbeitungszwecke beschränkt
- Zudem wurden weitere Vorgaben für die Verarbeitung durch empfangende Stellen eingefügt.

Die Regelung des § 31 im Niedersächsischen Schulgesetz ist im Ergebnis zwar sehr umfangreich ausgefallen, erfüllt nun aber den europarechtlichen Grundsatz der Erforderlichkeit und bietet den verantwortlichen Stellen in übersichtlicher Form umfassende Rechtssicherheit.

G.6. Neufassung des Kita-Gesetzes

Die Landesregierung beabsichtigt, das Gesetz über Tageseinrichtungen für Kinder (Kita-Gesetz) neu zu fassen. Da der Referentenentwurf eine umfassende Regelung zur Datenverarbeitung vorsah, wurde meine Behörde frühzeitig um eine Stellungnahme gebeten. Ich habe allerdings festgestellt, dass das Land keine Gesetzgebungskompetenz für datenschutzrechtliche Regelungen im Kita-Gesetz hinsichtlich der Daten von Kindern und Erziehungsberechtigten hat.

Diese Feststellung ergibt sich daraus, dass es sich bei den in Tageseinrichtungen verarbeiteten Daten um Sozialdaten handelt (§ 67 Abs. 2 Sozialgesetzbuch (SGB) X i.V.m. § 35 SGB I). Angebote zur Förderung von Kindern in Tageseinrichtungen sind Leistungen der Jugendhilfe. Mithin gilt das SGB VIII.

Das Kita-Gesetz beruht auf der Öffnungsklausel des § 26 SGB VIII. Demgemäß dürfen zwar Inhalt und Umfang der Aufgaben und Leistungen durch Landesrecht geregelt werden. Dies gilt jedoch nicht für datenschutzrechtliche Regelungen, da die Verarbeitung von Sozialdaten abschließend im zweiten Kapitel des SGB X und den weiteren Büchern des Sozialgesetzbuches geregelt wird.[1]

Nur Aufgaben und Leistungen Sache des Landesrechts

Spezialgesetzliche Regelung für Sozialdaten

Der Schutz der Sozialdaten, also der Daten von Kindern und deren Erziehungsberechtigten, wird in den §§ 61 ff SGB VIII spezialgesetzlich geregelt. Unmittelbare Geltung erlangen diese Normen für die Träger der öffentlichen Jugendhilfe und die Gemeinden.[2] Dagegen gelten sie nicht für die Träger der freien Jugendhilfe; vielmehr sind mit diesen Vereinbarungen abzuschließen, die ein entsprechendes Datenschutzniveau gewährleisten.[3]

Da der Bund durch das SGB VIII auf dem Gebiet der Kinder- und Jugendhilfe von der ihm zustehenden konkurrierenden Gesetzgebungskompetenz[4] im Bereich des Datenschutzes (durch die §§ 61 ff SGB VIII) abschließend Gebrauch gemacht hat, besteht bezüglich der öffentlichen Stellen keine Landeskompetenz.

Für die nicht-öffentlichen Stellen (also freie Träger) besteht ohnehin keine Landeskompetenz, stattdessen gelten die Vorschriften des Bundesdatenschutzgesetzes sowie der Datenschutz-Grundverordnung.

Ich habe das Kultusministerium über diese Rechtslage informiert. Das Gesetzgebungsverfahren war bei Redaktionsschluss noch nicht abgeschlossen. Auch eine Reaktion auf meine Stellungnahme lag bis dahin nicht vor.

1 gem. § 35 Abs. 2 SGB I

2 § 61 Abs. 1 SGB VIII.

3 § 61 Abs. 3 SGB VIII.

4 Kompetenztitel „öffentliche Fürsorge" nach Art. 74 Abs. 1 Nr. 7 GG

G.7. Änderung des Niedersächsischen Glücksspielgesetzes

Im Zuge der Reform des Niedersächsischen Glücksspielgesetzes soll ein Spielersperrsystem in Spielhallen eingeführt werden. Dabei fehlt es allerdings an Übermittlungsbefugnissen für Dritte an das Fachministerium, das über Fremdsperren entscheidet.

Die Niedersächsische Landesregierung hat den Entwurf einer Änderung des Niedersächsischen Glücksspielgesetzes am 23. Oktober 2019 in den Landtag eingebracht. Dieser sieht unter anderem die Einführung eines landesweiten Spielersperrsystems für Spielhallen vor. Der Entwurf orientiert sich am Glücksspielstaatsvertrag und am Hessischen Glücksspielgesetz.

Meine Behörde konnte wichtige Aspekte in den Gesetzentwurf einbringen. So wurde sichergestellt, dass die Entscheidung über eine Fremdsperre (beantragt durch Angehörige eines Spielsüchtigen/ eines Spielsuchtgefährdeten) durch das Wirtschaftsministerium getroffen wird und dieser Sperre Verwaltungsaktqualität zugemessen wird. Dies hat wichtige Auswirkungen auf die Verfahrensrechte der Betroffenen, wie beispielsweise die vorherige Anhörungspflicht.

Fremdsperre ist Verwaltungsakt

Mindestmaßnahmen für Sperrsystem

Zudem gelten die Regelungen der Datenschutz-Grundverordnung (DS-GVO), beispielsweise für die erforderlichen technisch-organisatorischen Maßnahmen zum Schutz der verarbeiteten Daten. Diese richten sich insbesondere nach den mit der Datenverarbeitung verbundenen Risiken für die Grundrechte der betroffenen Personen. Nähere Konkretisierungen sieht § 17 des Niedersächsischen Datenschutzgesetzes (NDSG) für den öffentlichen Bereich vor: Demnach sind als Mindestmaßnahmen im Spielersperrsystem vorzusehen:

- Die Etablierung eines Rechte-Rollenkonzeptes,
- die Protokollierung der jeweiligen Zugriffe,
- die Sensibilisierung und Schulung der Personen, die Zugriff auf das Sperrsystem haben
- sowie die Verschlüsselung zur Gewährleistung der Vertraulichkeit des elektronischen Systems.

Datenschutz-Folgenabschätzung nötig

Zudem ist es erforderlich eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO durchzuführen, da im Rahmen des Spielersperr-systems eine umfangreiche Verarbeitung von sensitiven Daten erfolgt. Dabei ist es unerheblich, dass die Gründe für die Sperre nicht in die Sperrdatei eingetragen

werden. Denn es wird dort zumindest festgehalten, ob eine Selbst- oder eine Fremdsperre vorliegt. Die Fremdsperre ist ein mittelbarer Hinweis auf eine Spielsuchtgefährdung und gilt damit als besonders zu schützendes Gesundheitsdatum.

Keine Übermittlungsbefugnisse für Dritte

Im Gesetzesvollzug wird sich die Frage stellen, wie die Meldungen zur Fremdsperre, z. B. durch Verwandte oder Bekannte von Spielsüchtigen oder Spielsuchtgefährdeten, an das Ministerium erfolgen sollen. Denn meiner Einschätzung nach bestehen hierfür keine Übermittlungsbefugnisse. Die Spielsuchtgefährdung darf als Gesundheitsdatum nur unter den engen Voraussetzungen des Art. 9. Abs. 2 DS-GVO verarbeitet werden. Auch das Übermitteln von personenbezogenen Informationen stellt eine Datenverarbeitung dar.

Petitionsrecht nicht geeignet

Unzutreffend ist die in der Gesetzesbegründung niedergelegte Auffassung, wonach das Petitionsrecht aus Artikel 17 des Grundgesetzes eine Befugnis zur Datenübermittlung für dritte Stellen beinhaltet. Denn das Petitionsrecht gilt stets nur in eigener Sache und kann die Vorgaben der DS-GVO nicht aushebeln.

Auch kann der Landesgesetzgeber diese Rechtsgrundlagen im Hinblick auf nicht-öffentliche Stellen und meldende Privatpersonen nicht schaffen, da hierfür ausschließlich der Bundesgesetzgeber zuständig ist.

Einwilligungen der Betroffenen notwendig

Die in der Praxis belastbarste und damit maßgebliche Feststellung einer Spielsucht wird eine ärztliche Diagnose sein. Als Berufsgeheimnisträger unterliegen Ärzte aber der Schweigepflicht. Entsprechende Datenübermittlungen sind wegen des strafrechtlich geschützten Patientengeheimnisses somit nur auf der Basis expliziter Einwilligungen der Betroffenen zulässig.

Öffentliches Interesse bei Spielsucht gegeben

Keine Bedenken habe ich hingegen bei der Entscheidungskompetenz des Ministeriums über die Fremdsperre. Denn über die Öffnungsklausel des Art. 9 Abs. 2 lit. g DS-GVO wird die gesetzliche Rechtsgrundlage für eine Verarbeitungsbefugnis geschaffen. Das erforderliche „erhebliche öffentliche Interesse“ kann bei einer nachgewiesenen Spielsucht bejaht werden.

Letztlich kann das vorgesehene Spielersperrsystem für Spielhallen jedoch nur der erste Schritt auf dem Weg zu einer umfassenden länderübergreifenden Lösung im Sinne eines einheitlichen und spielartenübergreifenden Glücksspielstaatsvertrages sein.

G.8. Vorbereitungen auf den Zensus 2021

Damit Gesetze und Planungen des Staates möglichst passgenau gestaltet werden können, wird alle zehn Jahre eine umfangreiche Statistische Erhebung unter der Bevölkerung, die sogenannte Volkszählung durchgeführt. Sie geht im kommenden Jahr mit dem Zensus 2021 in eine neue Runde. Bei der Vorbereitung waren zahlreiche Datenschutzbestimmungen zu beachten.

Der Begriff Volkszählung ist eng verbunden mit einem Meilenstein des Datenschutzrechts, dem Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983. Mit diesem Richterspruch wurde das Recht auf informationelle Selbstbestimmung etabliert, das aus der Menschenwürde des Artikel 1 Grundgesetz folgt. Das Bundesverfassungsgericht machte dem Gesetzgeber damit etliche Vorgaben, die bei einer Volkszählung zu beachten sind. So muss die Zweckbestimmung der Befragung ausdrücklich gesetzlich geregelt sein, die Ergebnisse dürfen nur zu statistischen Zwecken genutzt werden – und nicht für Einzelfälle wie z. B. einer Korrektur des Melderegisters. Außerdem forderte das Bundesverfassungsgericht, dass der Gesetzgeber organisatorische und verfahrensrechtliche Vorkehrungen festlegt, um die Vertraulichkeit und die Begrenzung auf Statistikzwecke zu sichern.

Informationen zum Urteil von 1983: https://t1p.de/volkszaehlung

Das Zensusgesetz 2021

Für den kommenden Zensus 2021 liegen auf Bundesebene die gesetzlichen Grundlagen vor. Ergänzend zum Zensusvorbereitungsgesetz 2021 wurde im Dezember 2019 das Zensusgesetz 2021 erlassen. Die wesentlichen Regelungen sind damit geschaffen. Der Zensus 2021 ist – im Gegensatz zur Volkszählung vor 30 Jahren – nicht als Totalerhebung (bei der alle Bürgerinnen und Bürger direkt befragt werden) vorgesehen. Vielmehr stützt sich der Zensus 2021 – wie auch bei der vorherigen Volkszählung – vor allem auf bereits bestehende Verwaltungsregister wie die Melderegister der Kommunen. Eine Haushaltsbefragung wird nur noch ergänzend stichprobenartig durchgeführt. Auch diese dient nur statistischen Zwecken und nicht einer etwaigen Korrektur des Melderegisters. Zusätzlich werden alle privaten Eigentümer von Wohnungen befragt. Und schließlich gibt es Befragungen in Wohnheimen und Gemeinschaftsunterkünften.

Zensusgesetz 2021: https://t1p.de/zensus2021

Es besteht eine Auskunftspflicht, die in § 23 Zensusgesetz 2021 geregelt ist. Der Gesetzgeber hat jedoch ausdrücklich festgeschrieben, dass personenbezogene Daten, wie Name und Geburtsdatum nur als Hilfsmerkmale verwendet werden dürfen.[1] Das bedeutet, dass diese Daten zunächst miterhoben werden, aber zum frühestmöglichen Zeitpunkt von den Erhebungsmerkmalen, für die der Zensus durchgeführt wird, getrennt werden. Die Hilfsmerk-

1 § 13 Absatz 2 Zensusgesetz 2021

male, dienen nur dazu, um in einem Übergangszeitraum die eigentlichen Erhebungsmerkmale auf Schlüssigkeit und Vollständigkeit prüfen zu können. Die personenbezogenen Daten sind dann zu löschen, wenn der statistische Zweck erreicht wurde, in jedem Fall aber vier Jahre nach dem Zensusstichtag.

Der Bundesgesetzgeber hat seine Hausaufgaben gemacht

Volkszählungsurteil ist umgesetzt

Seit dem Volkszählungsurteil hat sich viel getan. Der Gesetzgeber hat mittlerweile seine Hausaufgaben gemacht. Vor allem sind die vom Bundesverfassungsgericht 1983 geforderten organisatorischen und verfahrensrechtlichen Vorkehrungen zur Absicherung der Vertraulichkeit und der alleinigen Verwendung zu Statistikzwecken ausdrücklich im Gesetz festgeschrieben. Insbesondere sind die Erhebungsbeauftragten verpflichtet, die Unterlagen unverzüglich der Erhebungsstelle auszuhändigen.[2] Die Mitarbeiterinnen und Mitarbeiter in den Erhebungsstellen sind gesetzlich zur Geheimhaltung verpflichtet. Zudem müssen die Erhebungsstellen räumlich, organisatorisch und personell von anderen Verwaltungsstellen getrennt sein.[3]

Die vom Bundesgesetzgeber geschaffenen Grundlagen des Zensus 2021 sind aus Sicht des Datenschutzes unbedenklich. Auch die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) sind beachtet worden.

Datenschutz-Folgenabschätzung nicht im Bundesgesetz

Da das Zensusgesetz 2021 auch die Rechte der einzelnen Bundesländer berührt, hatte ich den Bundesbeauftragten für den Datenschutz (BfDI) gebeten, in seine Stellungnahme zum Zensusgesetz die Forderung nach einer Datenschutz-Folgenabschätzung (DSFA) auf Grundlage des Art. 35 Abs. 10 DS-GVO aufzunehmen. Eine solche zentrale DSFA hätte zu einer bundesweit einheitlichen Handhabe und zu einer erheblichen Entlastung der einzelnen Landesstatistikbehörden geführt.

Die Forderung wurde vom BfDI in seiner Stellungnahme zum Zensusgesetz 2021 aufgegriffen und hat Eingang in die Stellungnahme des Bundesrats zum Zensusgesetz gefunden. Die Bundesregierung lehnte sie allerdings ab. Als Grund wurde angegeben, dass die Nutzung einer DSFA zu einer künstlichen Aufspaltung isolierter Datenverarbeitungsschritte und zu einer Verschiebung des Kompetenzgefüges zwischen Bund und Ländern führen würde.

Ausschluss der Betroffenenrechte im ergänzenden Landesrecht

Bei Redaktionsschluss dieses Berichts befand sich das Niedersächsische Ausführungsgesetz zum Zensusgesetz 2021 in Vorbereitung. Der Entwurf sieht vor, dass gemäß der entsprechenden Öffnungsklausel[4] die Betroffenenrechte auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch im Rahmen des Zensus 2021 ausgeschlossen sind. Diese Einschränkungen der Betroffenenrechte mögen auf den ersten Blick irritieren. Allerdings sind sie zulässig, da die Rechte der Betroffenen durch die gesetzlichen Garantien, insbesondere durch die frühestmögliche Anonymisierung, gewahrt sind. Weitere Schwerpunkte des Niedersächsischen Ausführungsgesetzes sind Detailregelungen zu den Erhebungsbeauftragten und zur personellen, organisatorischen und räumlichen Abschottung der Erhebungsstellen. Ich bin hierbei frühzeitig eingebunden gewesen und habe keine datenschutzrechtlichen Bedenken gegenüber dem aktuellen Gesetzesentwurf.

Keine Bedenken gegenüber Gesetzesentwurf

Bei der Umsetzung des ergänzenden Landesrechts wird es darauf ankommen, dass die vorgeschriebene Abschottung der Erhebungsstellen strikt eingehalten wird. Ich werde mich daher mit dem Landesamt für Statistik in regelmäßigen Abständen austauschen.

2 § 20 Absatz 5 ebd.

3 § 19 Abs. 2 ebd.

4 Art. 89 Abs. 2 DS-GVO

H. Aufklärung / Schulung / Öffentlichkeitsarbeit

H.1. Vorträge für Bürgermeister, Vereine, Unternehmen und mehr

Seit meinem Amtsantritt ist es mein Ziel, die Behörde der Landesbeauftragten und deren Arbeit nach außen sicht- und wahrnehmbarer zu machen. In diesem Zusammenhang möchte ich mit den unterschiedlichen Zielgruppen meiner Tätigkeit ins Gespräch und in den Austausch kommen. Ein wichtiger Bestandteil sind dabei Vorträge und Diskussionsrunden zu verschiedenen Anlässen. Im vergangenen Jahr nahm ich selbst mehr als 40 solcher Termine wahr. Hinzu kommen zahlreiche Vorträge meiner Mitarbeiterinnen und Mitarbeiter.

Veranstaltungen für Vereine

Besonders stark verunsichert durch die Neuerungen der Datenschutz-Grundverordnung (DS-GVO) waren ehrenamtlich geführte Vereine. Ich habe diese deshalb u.a. durch eine Beratungs-Hotline unterstützt (siehe auch Kapitel H.4, S. 82). Sehr gern kam ich außerdem der Bitte zweier Landtagsabgeordneter nach, in deren Wahlkreisen Vorträge zum Datenschutz im Verein zu halten. Anfang bzw. Ende Mai traf ich in Bad Salzdetfurth und Bad Fallingbostel zahlreiche Ehrenamtliche, um darüber zu sprechen, was sich mit der DS-GVO tatsächlich für sie geändert hatte. Zu beiden Veranstaltungen begleitete mich jeweils eine Mitarbeiterin aus dem für Vereine zuständigen Fachreferat. So konnten im Rahmen dieser Zusammenkünfte viele, zum Teil auch sehr detaillierte Fragen diskutiert und beantwortet werden.

Gespräche mit Verbänden und Branchen

Eine weitere Zielgruppe, deren Informationsbedarf seit Geltung der DS-GVO sehr hoch war, waren Wirtschaftsunternehmen verschiedener Branchen und Größen. Diese fragten sich besonders, wie die Aufsichtsbehörden mit dem stark erweiterten Sanktionsrahmen der Verordnung umgehen würden. Bußgelder im Millionenbereich waren nun möglich, doch würde meine Behörde sie auch verhängen? Um dieses Informationsbedürfnis zu befriedigen, sprach ich u.a. im November im Rahmen einer Veranstaltung der Unternehmerverbände Niedersachsen (UVN) über die neue Rolle der Aufsichtsbehörden. Dabei

stellte ich immer wieder heraus, dass die Arbeit meines Hauses von einem Zweiklang bestimmt wird: Kontrolle und Vollzug auf der einen sowie Aufklärung, Information und Sensibilisierung auf der anderen Seite.

Zweiklang zwischen Kontrolle und Information

Dem zuletzt genannten Aufgabenbereich ordne ich auch eine Veranstaltungsreihe zu, die ich im vergangenen Jahr ins Leben gerufen habe. Dabei lade ich mehrere Unternehmen einer Branche zum Austausch ein, um über datenschutzrechtliche Herausforderungen der Gegenwart und Zukunft zu sprechen. Dadurch erhalte ich die Möglichkeit, dem in Art. 57 Abs. 1 lit. i DS-GVO normierten Anspruch an die Aufsichtsbehörden Rechnung zu tragen, nämlich maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Maßnahmen auswirken. Zugleich bieten diese Gespräche eine Gelegenheit, aufsichtsbehördliche Erwartungen und Positionen in einem größeren Kreis zu transportieren. Häufig entsenden die Unternehmen sowohl Vorstandsvertreter als auch Datenschutzbeauftragte zu diesen Terminen, wodurch es möglich ist, in der Diskussion verschiedene Perspektiven zu betrachten.

Bürgermeister-Konferenzen und Städteversammlung

Meine Befragung von 150 niedersächsischen Kommunen hat deutlich gezeigt, dass diese zum Geltungsbeginn der DS-GVO noch nicht alle Anpassungsarbeiten beendet hatten (siehe auch J.3.1, S. 125). Entsprechend groß war der Wunsch zum Austausch von kommunaler Seite. So nahm ich gerne die Einladung des Niedersächsischen Städte- und Gemeindebundes (NSGB) an und besuchte im März mehrere Bürgermeister-Frühjahrskonferenzen. Um alle sechs Termine des NSGB bedienen zu können, wurde ich dabei von den Beschäftigten des zuständigen Fachreferats unterstützt.

Ergebnisse der Kommunalprüfung: https://t1p.de/bericht-kommunen

Auch im Rahmen der Städteversammlung in Lüneburg hielt ich im September einen Vortrag zum Datenschutz im kommunalen Bereich. Genauso wie auf der Kommunalen Fachtagung des Niedersächsischen Studieninstitutes (NSI) Ende November. Das NSI hatte meine Kommunalprüfung zum Hauptthema der gesamten Tagung gemacht, weshalb ich dort auch noch detailliert auf die Arbeit meiner Behörde eingehen konnte.

Fachvortrag vor internationalem Publikum

Zu den genannten Terminen kommen zahlreiche weitere vor den verschiedensten Zielgruppen hinzu. Einen wichtigen Part nehmen dabei auch die Vorträge vor Fachpublikum ein, die ich im Rahmen von Datenschutzkongressen und -Workshops gehalten habe. Herausheben möchte ich dabei zum einen die Veranstaltung der „International Association of Privacy Professionals" (IAPP) im September in München. Die IAPP (mit Sitz in den USA) ist die laut eigenen Angaben weltweit größte Vereinigung von im Datenschutz beruflich tätigen Personen. Ihre Veranstaltungen bieten daher stets eine hervorragende Gelegenheit, sich über internationale Entwicklungen auszutauschen und zugleich die Situation in Europa zu beleuchten. Auf dem „Data Protection Intensive" in München durfte ich ausführlich über das Instrument der Datenschutz-Folgenabschätzung aus Sicht der Aufsicht sprechen.

Folgenabschätzung aus Perspektive der Aufsicht

Ebenfalls erwähnen möchte ich schließlich noch das Dialogforum der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), das im Juni in Hannover stattfand. In dieser Veranstaltungsreihe kommen regelmäßig Datenschutzverantwortliche mit Vertretern der Aufsichtsbehörden zusammen, um über deren Praxis sowie über Rechtsfragen bei der Umsetzung der DS-GVO zu diskutieren.

Es ließen sich noch viele weitere Veranstaltungen anführen, was allerdings den Rahmen dieses Berichts sprengen würde. So sollen die genannten Termine zumindest einen groben Überblick über die Bandbreite meiner Aktivitäten im Bereich von Information und Sensibilisierung geben.

H.2. Datenschutz geht zur Schule

Wer sieht, was ich online veröffentliche? Welche meiner Daten brauchen Apps wirklich? Wie wehre ich mich gegen Cyber-Mobbing? Diese und weitere Themen diskutierten Mitarbeiter meiner Behörde mit Schülern während einer Aktionswoche rund um den Safer Internet Day am 5. Februar. Dabei kooperierten neben Niedersachsen weitere Aufsichtsbehörden aus drei Bundesländern mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD).

Kinder und Jugendliche verbringen täglich viel Zeit im Internet und in den sozialen Medien. Daher ist es besonders wichtig, sie für die Risiken zu sensibilisieren, die mit der Nutzung von Online-Angeboten verbunden sein können.

Vorträge für 800 Jugendliche

Meine Mitarbeiterinnen und Mitarbeiter besuchten in der Zeit vom 4. bis 8. Februar neun Schulen, unter anderem in Lüneburg, Osnabrück, Hannover, Helmstedt, Hildesheim und Göttingen. Dabei erreichten sie mehr als 800 Schülerinnen und Schüler der 7. und 8. Klasse. In ihren Vorträgen griffen die Referenten auf die Unterlagen der BvD-Aktion „Datenschutz geht zur Schule“ zurück. Mit dieser Initiative zeigt der BvD seit 2009 Schülerinnen und Schüler einfache Wege auf, wie sie ihre persönlichen Daten besser schützen können, ohne dabei auf moderne Kommunikationsformen verzichten zu müssen.

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

Hier waren die LfD-Mitarbeiter im Einsatz.

Die Unterrichtsmaterialien wurden zuvor mit Unterstützung der EU-Initiative „klicksafe“ und der DATEV-Stiftung weiterentwickelt. Verbunden mit der jahrelangen Praxiserfahrung der ehrenamtlichen BvD-Referenten ist so eine profunde Unterrichtsgrundlage entstanden, die sich speziell an Kinder und Jugendliche richtet.

Aktion wird fortgesetzt

Die positive Resonanz von Schülern und Lehrkräften sowie die guten Eindrücke, die meine Mitarbeiterinnen und Mitarbeiter gewinnen konnten, haben den Ausschlag dafür gegeben, dass sich meine Behörde auch in den kommenden Jahren an der Aktion des BvD beteiligen wird. Ziel wird es sein, noch mehr Jugendliche zu erreichen. Denn nur wenn sich Jugendliche der potenziellen Risiken bei der Nutzung der vielfältigen digitalen Angebote bewusst sind, sind sie auch in der Lage den persönlichen Wert ihrer Daten abzuwägen und zu entscheiden, wie viel sie von sich preisgeben wollen.

H.3. Datenschutzinstitut Niedersachsen

Auch 2019 wurden die Kurse des Datenschutzinstituts Niedersachsen (DsIN) sehr gut von den Beschäftigten des öffentlichen Dienstes angenommen. Doch angesichts steigender Aufwände in der Vollzugspraxis meines Hauses kommt das DsIN nur in sehr geringem Umfang zum Einsatz. Eine deutliche Erhöhung der Kapazitäten sowie Ausweitung von Zielgruppen und Schulungsorten wäre nicht nur wünschenswert. Sie wäre auch erforderlich, um dem Auftrag der DS-GVO zu Sensibilisierung von Verantwortlichen und Öffentlichkeit Rechnung zu tragen. Doch dazu wäre deutlich mehr Personal nötig.

Basiskurs am besten besucht

Die meisten Teilnehmer besuchten 2019 den Basiskurs „Grundlagen des Datenschutzrechts für öffentliche Stellen". In dem Seminar werden Themen wie die Grundsätze der Datenverarbeitung, die Auftragsverarbeitung, die Betroffenenrechte oder technisch-organisatorische Pflichten vorgestellt. Anhand praxisorientierter Beispiele erfahren die Teilnehmer, welche Konsequenzen die Regelungen zum Datenschutz haben und welche Maßnahmen in den einzelnen Organisationseinheiten getroffen und regelmäßig überprüft werden müssen.

Gestaltung von Webseiten

Neben weiteren, bewährten Angeboten, z. B. zum technisch-organisatorischen Datenschutz, Datenschutz in der Schule und im Sozialbereich, hatte das DsIN auch einen neuen Kurs im Programm: „Datenschutzkonforme Gestaltung von Webseiten". Da der Internetauftritt ein wichtiger Bestandteil der Öffentlichkeitsarbeit nahezu jeder öffentlichen Stelle ist, informierte dieses Seminar umfassend über die datenschutzrechtlichen Anforderungen bei Gestaltung und Betrieb einer Webpräsenz.

Mit Blick auf die zahlreichen verantwortlichen Stellen in Niedersachsen und deren hohen Informationsbedarf müsste das Angebot des DsIN massiv erweitert werden. Mein Anspruch ist es, Schulungen nicht nur zentral in Hannover, sondern in ganz Niedersachsen anzubieten. Damit einhergehend sollte die Zahl der Teilnehmer deutlich erhöht werden, auch die Ansprache weiterer Zielgruppen wäre wünschenswert. Ob sich diese Pläne realisieren lassen, hängt aber ganz maßgeblich von der organisatorischen und personellen Weiterentwicklung meines Hauses ab.

H.4. Datenschutz im Verein

Rund um den Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) war eine deutliche Verunsicherung spürbar, auch und gerade in Vereinen. Meine Behörde hat deshalb in den vergangenen gut eineinhalb Jahren viel getan, um spezielle Beratungsangebote für den ehrenamtlichen Bereich zu schaffen. So wurden interessierte Verbände in eigenen Schulungen über die Neuerungen der DS-GVO und deren Umsetzung in den Vereinen informiert.

Vielen Vereinen wurde offenbar erst mit dem Wirksamwerden der DS-GVO die datenschutzrechtliche Relevanz ihrer Arbeit bewusst. Unter anderem die verstärkte mediale Berichterstattung machte viele Verantwortliche aufmerksam. Daher erreichten mich ab dem ersten Quartal 2018 vermehrt Anfragen zu Informationsveranstaltungen und Beratungsangeboten.

Angebote der Aufsichtsbehörde

Handreichung „Datenschutz im Verein": https://t1p.de/ds-vereine

Soweit es die personellen Möglichkeiten zuließen, kam meine Behörde den Anfragen und Wünschen nach. Zudem stellte ich auf meiner Webseite grundlegende Informationen für Vereine bereit. So bietet beispielsweise die Handreichung „Datenschutz im Verein" einen Überblick über die wichtigsten Anforderungen des neuen Datenschutzrechts.

Darüber hinaus enthält meine Internetseite Erläuterungen zur Bestellung von Datenschutzbeauftragten in Vereinen, Informationen für Betreiber von Webseiten sowie Hinweise zur Veröffentlichung von Fotografien. Zusätzlich richtete ich ab November 2018 an drei Vormittagen der Woche eine Vereins-Hotline ein. Dieses Angebot zur telefonischen Beratung besteht nach wie vor.

Forderungen der Landespolitik

Entschließungsantrag im Landtag

Die Unsicherheit in den Vereinen führte auf Initiative der Fraktionen von CDU und SPD dazu, dass sich auch der Niedersächsische Landtag mit dem Thema auseinandersetzte. Im Entschließungsantrag „Ehrenamt stärken - Datenschutz-Grundverordnung für Vereine handhabbar machen!" wurde meine Behörde um eine bestmögliche Beratung der Vereine gebeten. Zudem wurde ich ersucht, den Grundsatz „Beratung vor Sanktion" zu befolgen sowie eine anwenderfreundliche und konkrete Handreichung für die Vereine in Niedersachsen zu erarbeiten.

Am 10. Januar 2019 bekam meine Behörde Gelegenheit, im Innenausschuss des Landtages zum Entschließungsantrag Stellung zu nehmen. Dabei erläuterte mein Stellvertreter, Dr. Christoph Lahmann, inwiefern meine Behörde im Rahmen ihrer personellen Möglichkeiten Beratung anbietet. Darüber hinaus verdeutlichte er die bereits vor den Forderungen aus der Politik gelebte Praxis meines Hauses, wonach in Bezug auf Vereine grundsätzlich Hinweise und Be-

ratung Vorrang vor Bußgeldern haben. Die Festsetzung eines Bußgeldes ist das letzte Mittel der Wahl, zumal die Aufsichtsbehörden mit der DS-GVO noch weitere Abhilfebefugnisse haben, wie etwa die Warnung und die Verwarnung.

Bußgelder als letztes Mittel

Das heißt aber nicht, dass Erstverstöße nicht auch ein Bußgeld nach sich ziehen können. Auch die Mitglieder von Vereinen haben einen Anspruch darauf, dass rechtskonform mit ihren Daten umgegangen wird. Grundsätzlich sind deshalb auch im ehrenamtlichen Bereich Sanktionen möglich, sofern gravierende Datenschutzverstöße festgestellt werden.

Zwar sieht die DS-GVO die individuelle Beratung nicht als explizite Aufgabe der Aufsichtsbehörden vor. Dennoch ist mir die Unterstützung der vielen Menschen, die sich ehrenamtlich engagieren, ein wichtiges Anliegen. Daher bin ich der Anfrage zweier Landtagsabgeordneter gerne nachgekommen und habe im Mai 2019 Informationsveranstaltungen in den jeweiligen Wahlkreisen durchgeführt (siehe auch H.1, S. 76). Auf diesem Weg konnte ich in den unmittelbaren Austausch mit den Verantwortlichen in den Vereinen treten, Näheres über deren Herausforderungen und Nöte erfahren sowie manche Fragen direkt beantworten.

Veranstaltungen für Vereine mit MdL

Änderungen im Datenschutzgesetz

Von den Vereinen sehr begrüßt wurde eine Gesetzesänderung im vergangenen Jahr, wonach die Bestellpflicht für Datenschutzbeauftragte erst ab einer Zahl von 20 Personen gilt, die ständig automatisiert personenbezogene Daten verarbeiten. Vorher galt die Bestellpflicht bereits ab einer Zahl von zehn Personen (siehe dazu auch Kapitel E.3, S. 37). Die Initiatoren der Gesetzesänderung gaben an, besonders kleine Unternehmen und Vereine entlasten zu wollen.

Aufweichung der Bestellpflicht von Datenschutzbeauftragten

Ich habe mich – im Einvernehmen mit den anderen deutschen Aufsichtsbehörden – ausdrücklich dagegen ausgesprochen, bestehende Regelungen zu verwässern oder abzuschaffen. Auch wenn viele Vereine nun nicht mehr unter die Bestellpflicht fallen, bleiben die übrigen Vorgaben des Datenschutzrechts für sie bestehen. Der Unterschied liegt allerdings darin, dass die Vereine diese nun ohne die Fachkompetenz eines eigenen Datenschutzbeauftragten erfüllen müssen.

Umsetzung der DS-GVO in den Vereinen

Die Zahl der Anrufe an der Vereins-Hotline meiner Behörde ist inzwischen rückläufig. Dennoch besteht weiterhin Beratungsbedarf bei den Vereinen, vergleichbar mit dem Bedarf von Kleinunternehmen. Die Fragen betreffen insbesondere die Informationspflichten nach Art. 13 und 14 DS-GVO, die Umsetzung der Betroffenenrechte (z. B. das Auskunfts- und Löschungsrecht), die Gestaltung von Webseiten sowie die Veröffentlichung von Fotos. Ich habe daher zu diesen Themenkomplexen Handreichungen (FAQs) mit den Antworten auf die wichtigsten Fragen auf meiner Webseite veröffentlicht.

Fragen zu Infopflichten und Betroffenenrechten

Dass diese Angebote durchaus ihre Berechtigung haben, zeigt sich nicht nur an den entsprechenden Anfragen, sondern lässt sich auch aus den Beschwerden ableiten, die meine Behörde erreichen. Häufig beschweren sich Vereinsmitglieder, dass ihnen Auskünfte nicht ausreichend, nicht rechtzeitig oder überhaupt nicht erteilt worden seien. Daher möchte ich betonen, dass Grundlage einer sachgemäßen und umfassenden Auskunft ein ordnungsgemäßes Verzeichnis der Verarbeitungstätigkeiten ist. Eine einwandfreie Dokumentation ermöglicht es Vereinen, die Wahrung der Informations- und Auskunftspflicht nachzuweisen.

H.5. Veröffentlichung von Informationsmaterial

Ein wichtiger Teil der Aufklärungs- und Sensibilisierungsarbeit meines Hauses ist die Publikation von Informationsmaterialien auf meiner Webseite. Dieses Angebot wird beständig ausgebaut und aktualisiert, so auch im vergangenen Jahr.

FAQ zur Videoüberwachung: https://t1p.de/faq-video

Da meine Behörde regelmäßig sowohl Beschwerden als auch Beratungsanfragen zum Thema Videoüberwachung erreichen, erschien es geboten, das Informationsangebot hierzu auszuweiten. Deshalb habe ich die grundsätzlichen Fragen und die entsprechenden Antworten veröffentlicht, die sich im Zusammenhang mit Kameraüberwachung stellen. Diese sogenannten FAQ (Frequently asked questions) erläutern unter anderem, was man vor der Installation einer Kamera bedenken sollte und in welcher Form man auf diese hinweisen muss.

Deutlich erweitert wurde das Informationsangebot für Vereine. Bereits im Januar 2019 erschien eine Handreichung „Datenschutz im Verein“, die einen Überblick über die wichtigsten datenschutzrechtlichen Fragen im Vereinsleben geben soll. Darin enthalten sind neben Empfehlungen für die Datenschutzordnung des Vereins auch Hinweise zur Bestellung von Datenschutzbeauftragten, zur Meldung von Datenpannen und zur Erfüllung der Betroffenenrechte.

Handreichung „Datenschutz im Verein“: https://t1p.de/ds-vereine

FAQ im Sozialrecht und in der Kita

Obwohl im Sozialrecht und im Bereich der Kindertagesstätten durch die Datenschutz-Grundverordnung nur wenige Rechtsänderungen eingetreten sind, haben die Beratungsanfragen auch in diesen Bereichen stark zugenommen. Um den verantwortlichen Stellen und den Betroffenen einen Überblick über die wichtigsten Aspekte zu geben, habe ich auch hier die häufigsten Fragen und Antworten zusammengestellt.

Die FAQ zum Datenschutz in der Kita betreffen im Kern die Bereiche der Verarbeitungsbefugnisse und Aufbewahrungsvorschriften. Zudem werden Fragen zur Veröffentlichung von Fotos sowie zu weiteren Themenfeldern aufbereitet.

FAQ für Kitas: https://t1p.de/faq-kita

Die FAQ zum Datenschutz im Bereich der Gewährung von Arbeitslosengeld II umfassen die häufigsten Anfragen zu Verarbeitungs- und Übermittlungsbefugnissen, zur Vorlage von Kontoauszügen und zur Vermieterbescheinigung. Ebenfalls thematisiert werden die häufig eingeholten Schweigepflicht-Entbindungserklärungen.

Für weitere Bereiche des Sozialrechts werden zu gegebener Zeit zusätzliche FAQ erstellt. Auch in anderen Bereichen ist eine Erweiterung des Informationsangebots geplant. So sind als Folge der Querschnittsprüfung von Wirtschaftsunternehmen (siehe J.6.1, S. 142) mehrere Handreichungen zum technisch-organisatorischen Datenschutz in Arbeit. Weiterhin beabsichtige ich, FAQ zur Auftragsverarbeitung und Informationen zur Veröffentlichung von Fotos durch öffentliche Stellen zur Verfügung zu stellen.

FAQ zu Sozialrecht: https://t1p.de/faq-sozial

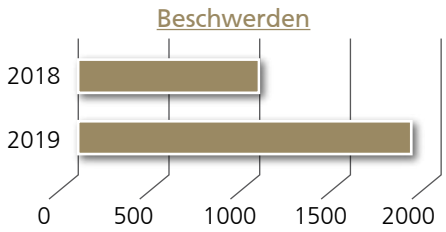
I. Aufsicht und Vollzug

I.1. Zahlen und Fakten

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

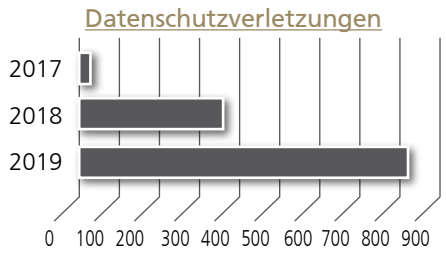
Beratungen

Aufgrund der stark gestiegenen Aufwände bei der Bearbeitung von Beschwerden und Meldungen von Datenschutzverletzungen musste ich die Beratungstätigkeit meines Hauses stark einschränken. Dennoch haben meine Mitarbeiterinnen und Mitarbeiter im Berichtszeitraum immer noch 1878 schriftliche Beratungen geleistet (hiervon sind auch Beratungen per E-Mail umfasst), obgleich die Beratung im Einzelfall als solche nicht mehr in der Datenschutz-Grundverordnung (DS-GVO) vorgesehen ist. Ausschließlich telefonische Beratungen werden hier ebenso wie Schulungen und Vorträge nicht berücksichtigt.



Beschwerden

Die Zahl der Beschwerden, die Betroffene gemäß Art. 77 DS-GVO bei der Aufsichtsbehörde einreichen können, bewegt sich bei der LfD Niedersachsen seit Geltung der Verordnung auf einem gleichbleibend hohen Niveau (siehe auch Kapitel I.2, S. 88). Gingen 2018 bereits etwas mehr als 1000 Beschwerden ein, weil sich die Betroffenen in ihren Rechten verletzt sahen, waren es 2019 insgesamt 1882.



Gemeldete Datenschutzverletzungen

Wie in Kapitel I.3 beschrieben (S. 93), müssen unter Geltung der DS-GVO weit mehr Datenschutzverletzungen gemeldet werden, als zuvor. Das hatte bereits 2018 zur Folge, dass sich die Meldungen gemäß Art. 33 DS-GVO auf 370 steigerten (gegenüber 20 im Jahr 2017). Dieser Trend hat sich 2019 fortgesetzt und noch weiter verstärkt. Im vergangenen Jahr meldeten Verantwortliche 824 Datenschutzverletzungen.

Abhilfemaßnahmen nach DS-GVO

Art. 58 Abs. 2 DS-GVO normiert die Liste der Abhilfebefugnisse, welche die Aufsichtsbehörden einsetzen können. Lag 2018 der Schwerpunkt meiner Tätigkeit noch sehr deutlich in der Beratung zur DS-GVO, habe ich im vergangenen Jahr vermehrt von diesen Befugnissen Gebrauch gemacht. So habe ich 5 Warnungen (Art. 58, Abs. 2 lit.a DS-GVO), 13 Anweisungen und Anordnungen (Art. 58, Abs. 2 lit. c-g und j) sowie 190 Verwarnungen (Art. 58, Abs. 2 lit.b DS-GVO) ausgesprochen.

Aufgrund von 22 Vorwürfen habe ich Geldbußen gem. Art. 58 Abs. 2 lit. i DS-GVO in Höhe von fast 480.000 Euro verhängt. Zum Ende des Berichtszeitraums war aber der ganz überwiegende Teil dieser Summe noch nicht rechtskräftig.

Europäische Verfahren

Eine der größten Errungenschaften und zugleich Herausforderungen der DS-GVO ist die Zusammenarbeit der Aufsichtsbehörden auf EU-Ebene. Bei grenzüberschreitenden Datenverarbeitungen verpflichtet die DS-GVO die Behörden dazu, in einem strukturierten Verfahren zusammenzuarbeiten und aufsichtsrechtliche Entscheidungen untereinander abzustimmen. Bei grenzüberschreitenden Fällen wird im Rahmen des One-Stop-Shop-Prinzips eine federführende Aufsichtsbehörde bestimmt, welche dann das aufsichtsrechtliche Entscheidungsverfahren koordiniert. Die Informationen zu den einzelnen Verfahren speisen die Aufsichtsbehörden in das Internal Market Information-System (IMI) ein. Im Jahr 2019 war mein Haus in folgendem Umfang mit europäischen Verfahren befasst:

1. Verfahren mit Betroffenheit (Art.56): **320**
2. Verfahren mit Federführung (Art. 56): **3**
3. Verfahren gem. Kap VII DS-GVO (Art. 60ff.):
   a. Verfahren mit Betroffenheit (Art. 60): **44**
   b. Verfahren mit Betroffenheit (Art. 60), in denen ein finaler Beschluss vorgelegt wurde: **31**
   c. Verfahren mit Federführung (Art. 60): **0**

Ressourcen der Behörde

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

I.2. Betroffene nutzen ihre Rechte – Beschwerden nehmen zu

Die Datenschutz-Grundverordnung hat die Rechte der Betroffenen bekanntlich gestärkt, darunter auch die Ansprüche von Beschwerdeführern. Die Frage lautete nun: Wie werden diese Möglichkeiten in der Praxis genutzt? Die Antwort: Die Bürger kennen ihr Beschwerderecht und nehmen es vielfach in Anspruch, um datenschutzrechtliche Fragestellungen zu klären.

1882 Beschwerden im Jahr 2019

Im Jahr 2019 erreichten mich insgesamt 1882 Beschwerden gemäß Artikel 77 Datenschutz-Grundverordnung (DS-GVO), darunter rund 1000 bezogen auf den nicht-öffentlichen Bereich. Die Bürger machen also von ihren Rechten rege Gebrauch, wenn sie den Verdacht haben, dass ihre Daten rechtswidrig verarbeitet wurden. Gegenstand der Beschwerden sind unterschiedliche Verdachtsmomente auf Verstöße gegen die zahlreichen Pflichten, welche die DS-GVO den Verantwortlichen aufgibt.

Doch nicht hinter jeder Beschwerde verbirgt sich auch tatsächlich ein Verstoß. Meine Behörde ermittelt deshalb zunächst den Sachverhalt und bewertet ihn im Anschluss datenschutzrechtlich. Hier bedarf es Fingerspitzengefühl, denn vielfach beruht der Grund der Beschwerde nicht nur auf datenschutzrechtlichen Unstimmigkeiten. Mitunter wird der Datenschutz auch als Vehikel genutzt, um arbeitsrechtliche, familiäre oder nachbarschaftliche Streitigkeiten auszutragen. Soweit ein Verstoß gegen die Bestimmungen der DS-GVO vorliegt, wählt meine Behörde ein geeignetes Aufsichtsmittel aus dem Katalog des Art. 58 Abs. 2 DS-GVO und stellt dem Verantwortlichen einen entsprechenden Bescheid aus. In einigen Fällen wird zudem ein Ordnungswidrigkeitenverfahren eingeleitet und ggf. ein Bußgeld verhängt. Liegt der Verdacht einer Straftat vor, wird das Verfahren an die Staatsanwaltschaft abgegeben.

Gründe für Beschwerden

Besonders häufig beziehen sich Beschwerden auf Verstöße gegen das Auskunftsrecht nach Art. 15 DS-GVO, auf eine unzulässige Videoüberwachung (siehe dazu auch Kapitel J.9, S. 169), den Fehlversand von Unterlagen oder den Erhalt eines Newsletters trotz Abbestellung (Kapitel J.6.3, S. 149). Auch der E-Mail-Versand mit offen einsehbarem CC-Verteiler sowie Verstöße gegen das Recht auf Löschung gemäß Art. 17 DS-GVO kommen regelmäßig vor. Schließlich erreichten meine Behörde auch Beschwerden wegen Verstößen gegen die Informationspflichten nach Art. 13 und 14 DS-GVO.

Auskunftsrecht nach Art. 15 DS-GVO

Immer wieder gehen Beschwerden darüber ein, dass Verantwortliche das Auskunftsrecht nach Art. 15 DS-GVO nicht beachten. Im nicht-öffentlichen Bereich ist dies der häufigste Beschwerdegrund. Laut den Beschwerdeführern werden Auskunftsbegehren von den Verantwortlichen oft nicht oder nicht

fristgemäß beachtet. Überdies haben die betroffenen Personen häufig den Eindruck, die Auskunft sei unvollständig.

Betroffener hat Anspruch auf zahlreiche Informationen

Nach Art. 15 Abs. 1 DS-GVO kann jede Person vom Verantwortlichen zunächst eine Bestätigung verlangen, dass dieser personenbezogene Daten verarbeitet, die sie betreffen. Trifft das zu, hat der Betroffene Anspruch auf Auskunft über diese personenbezogenen Daten sowie auf folgende Informationen:

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten, die verarbeitet werden,
- ggf. die Empfänger oder Kategorien von Empfängern,
- die geplante Speicherdauer oder die Kriterien für deren Festlegung,
- die Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung,
- das Widerspruchsrecht,
- das Beschwerderecht bei der Aufsichtsbehörde und
- ggf. die Herkunft der Daten sowie das Bestehen einer automatisierten Entscheidungsfindung (inkl. Profiling) nebst involvierter Logik, Tragweite und angestrebten Auswirkungen für die betroffene Person.

Angesichts des Umfangs der zu erteilenden Auskunft ist die Beantwortung eines Auskunftsersuchens fehleranfällig. Nach den Feststellungen meiner Behörde ergibt sich folgendes Bild: Viele Beschwerden sind begründet, da tatsächlich oft keine Auskunft erteilt, wurde. Unvollständige Auskünfte wurden dagegen nur in wenigen Fällen gegeben. Die Auskunft ist nicht auf Stammdaten beschränkt, sondern kann sich etwa auch auf Telefonvermerke oder Gesprächsnotizen beziehen, die zu dem Betroffenen angelegt wurden. Für die Erteilung der Auskunft gelten das Genauigkeits- und das Verständlichkeitsgebot aus Art. 12 Abs. 1 Satz 1 DS-GVO, was eine gewisse Aufbereitung oder Erläuterung erforderlich machen kann.

Zum Teil selbst festgelegte Fristen

Es gibt in diesem Bereich allerdings auch einige unbegründete Beschwerden. In diesen Fällen stellte meine Behörde entweder fest, dass der Verantwortliche die Auskunft erteilt hatte oder dass die Antwortfrist von einem bzw. von bis zu drei Monaten nach Art. 12 Abs. 3 DS-GVO noch nicht verstrichen war. Mit Blick auf die Auskunftsfrist haben Beschwerdeführer mitunter unrealistische Vorstellungen. Sie sind der Auffassung, der Verantwortliche habe binnen einer selbstgesetzten Frist von beispielsweise drei Tagen die gewünschte Auskunft zu erteilen.

Recht auf Kopie

Relevanz hat zudem das Recht auf Kopie gemäß Art. 15 Abs. 3 DS-GVO. Zur Frage, in welcher Form eine Kopie zur Verfügung zu stellen ist, besteht noch keine einheitliche Auslegung. Zum Teil wird die Ansicht vertreten, dass der Anspruch auf Kopie auch durch Überlassung einer strukturierten Zusammenfassung der verarbeiteten Daten erfüllt werden kann. Das überzeugt mich aber nicht. Nach allgemeinem Verständnis ist mit einer Kopie eine originalgetreue Reproduktion gemeint. Es wird also die Herausgabe der Informationen in der Form gefordert, in der sie dem Verantwortlichen vorliegen.

In der Praxis halte ich dennoch grundsätzlich ein gestuftes Verfahren für denkbar: Das heißt, der Verantwortliche könnte zunächst Auskünfte in Form aufbereiteter Daten erteilen. Bei einer großen Datenmenge kann der Verantwortliche zudem eine Präzisierung der erbetenen Auskunft verlangen (Erwägungsgrund 63). Fordert der Betroffene jedoch ausdrücklich eine Kopie seiner gesamten personenbezogenen Daten, muss der Verantwortliche dieser Forderung grundsätzlich nachkommen. Eine Begrenzung des Anspruchs erfolgt allerdings durch Rechte anderer Personen

sowie aufgrund etwaiger Geheimhaltungspflichten. Ich empfehle deshalb, sich mit dem Betroffenen darüber abzustimmen, wie und in welchem Umfang die Auskunft und die Erstellung der Kopie erfolgen sollen.

Schon die Anzahl von Beschwerden auf diesem Gebiet zeigt, dass vielen Bürgern der Schutz ihrer persönlichen Daten wichtig ist. Bedauerlicherweise ist noch nicht allen Verantwortlichen das Recht auf Auskunft bzw. dessen Umfang bekannt, weshalb hier weiterhin Aufklärungsbedarf besteht, flankiert von entsprechenden Kontrollen.

Recht auf Löschung gemäß Artikel 17 DS-GVO

Jede betroffene Person hat gemäß Art. 17 Abs. 1 DS-GVO grundsätzlich einen Anspruch auf Löschung ihrer personenbezogenen Daten. Dieses Recht besteht u.a., wenn die Daten nicht mehr notwendig sind (Zweckentfall), bei Widerruf der zugrundeliegenden Einwilligung, bei Fehlen einer Rechtsgrundlage für die Verarbeitung oder bei Bestehen einer gesetzlichen Löschpflicht.

Ausnahmen vom Recht auf Löschung

Ausnahmen des Rechts auf Löschung bestimmt Art. 17 Abs. 3 DS-GVO. Danach hat eine betroffene Person kein Recht auf Löschung ihrer personenbezogenen Daten, wenn die Verarbeitung erforderlich ist

- zur Wahrnehmung des Rechts auf freie Meinungsäußerung und Information,
- zur Erfüllung einer rechtlichen Verpflichtung,
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit,
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder statistische Zwecke i.S.v. Art. 89 Abs. 1, wenn die Löschung die v.g. Zwecke erheblich beeinträchtigt,
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Art. 17 Abs. 3 DS-GVO wird durch § 35 BDSG ergänzt. Findet dieser Anwendung, wandelt sich das Recht auf Löschung in ein Recht auf Einschränkung der Verarbeitung i.S.v. Art. 18 DS-GVO. Nach § 35 BDSG besteht in besonderen Ausnahmefällen bei nicht automatisierter Datenverarbeitung kein Löschanspruch, wenn dieser nur mit unverhältnismäßig hohem Aufwand bei zugleich geringem Interesse der betroffenen Person erfüllt werden kann. Weiter besteht eine Einschränkung des Löschrechts, wenn dadurch die Interessen der betroffenen Person beeinträchtigt werden sowie bezogen auf den Zweckentfall bei besonderen satzungsgemäßen oder vertraglichen Aufbewahrungsfristen.

Ausnahmen sind zeitlich begrenzt

Die Ausnahmen sind allerdings zeitlich beschränkt und berechtigen nicht zu einer unbegrenzten Verarbeitung. Unter die Ausnahme fallen insbesondere Aufbewahrungs- und Dokumentationspflichten, die sich aus dem allgemeinen Zivilrecht, aus dem Handels- sowie dem Steuerrecht ergeben. Danach müssen Unternehmen Unterlagen und damit auch personenbezogene Daten in der Regel sechs bzw. zehn Jahre aufbewahren.

Bisweilen wird die Auffassung vertreten, dass die Verschlüsselung von Daten mit deren Löschung gleichzusetzen sei. Diese Ansicht teile ich nicht. Durch eine Verschlüsselung wird nur die Vertraulichkeit der Daten geschützt. Dies ändert aber nichts an der Bewertung als personenbezogene Daten, zumal der Verantwortliche eine Entschlüsselung vornehmen kann. Je nach eingesetzter

Verschlüsselungstechnik und dem allgemeinen Stand der Technik besteht zudem das Risiko, dass auch Dritte eine Entschlüsselung vornehmen können.

Diese Ausführungen zeigen, wie komplex das Recht auf Löschung ist. Deshalb ist es wenig überraschend, dass es Gegenstand vieler Beschwerden ist. In einigen Fällen übersehen die Beschwerdeführer jedoch die handels- und steuerrechtlichen Aufbewahrungspflichten, die einer Löschung entgegenstehen. Außerhalb dieses Bereichs kamen die Verantwortlichen den Löschungsbegehren im Regelfall nach, konnten dieses aber nicht sofort erfüllen, sondern brauchten zeitlichen Vorlauf.

Auch hier wird deutlich: Die Betroffenen nehmen ihre Rechte wahr, sind sensibilisiert und wehren sich gegen die unrechtmäßige Verarbeitung ihrer personenbezogenen Daten.

Informationspflicht (Art. 13, 14 DS-GVO)

Jeder Verantwortliche unterliegt der Informationspflicht; entweder nach Art. 13 DS-GVO, wenn die Daten bei der betroffenen Person erhoben werden oder gemäß Art. 14 DS-GVO, wenn die Daten nicht bei der betroffenen Person erhoben werden.

Inhalt der Informationspflicht

Nach Art. 13 DS-GVO muss der Verantwortliche die betroffene Person über Folgendes informieren:

- Name und Kontaktdaten des Verantwortlichen sowie des Vertreters,
- ggf. Kontaktdaten des Datenschutzbeauftragten,
- Zwecke und Rechtsgrundlage der Datenverarbeitung,
- ggf. berechtigtes Interesse,
- Empfänger der Daten,
- bei Datentransfer in Länder außerhalb des Europäischen Wirtschaftsraums: Existenz oder Fehlen eines Angemessenheitsbeschlusses der EU-Kommission, geeignete Garantien (z. B. Standardverträge), ggf. Tatsache des Drittstaatenverkehrs und die Interessen des Verantwortlichen,
- Dauer der Speicherung bzw. Kriterien für deren Festlegung,
- Hinweis auf Auskunfts-, Berichtigungs-, Löschungs-, Einschränkungs- sowie Widerspruchsrecht und auf das Recht der Datenportabilität,
- bei Einwilligungen auf die Widerrufsmöglichkeit,
- Beschwerderecht bei der Aufsichtsbehörde,
- ob die Angabe der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsschluss notwendig ist und die Folgen einer Nichtangabe sowie
- bei automatischer Entscheidungsfindung das Vorhandensein an sich, eine aussagekräftige Darstellung der Entscheidungslogik sowie Tragweite und Konsequenz für die betroffene Person.

FAQ zu den Info-Pflichten: https://t1p.de/faq-info

Schließlich muss der Verantwortliche nach Art. 21 Abs. 4 DS-GVO über das Widerspruchsrecht gegen Direktmarketingmaßnahmen informieren.

Basisinformationen beim ersten Kontakt

Anders als in digitalen Umgebungen kann das Erfordernis der Information zum Erhebungszeitpunkt in bestimmten, nicht-digitalen (Alltags-)Situationen zu Fragen der praktischen Anwendung führen. Im Regelfall reicht es hier daher meiner Auffassung nach aus, wenn beim ersten Kontakt Basisinformationen, d.h., die Angaben zum Verantwortlichen, zum Zweck der Verarbeitung sowie

zu den Betroffenenrechten gegeben werden. Zu den weiteren Informationen kann der Verantwortliche auf seine Webseite verweisen oder ein entsprechendes Informationsblatt anbieten.

Meist wurde bei Beschwerden in diesem Bereich eine unzureichende Information gerügt, nur in wenigen Fällen unterblieb die Information ganz. Soweit meine Behörde im Rahmen der Sachverhaltsaufklärung tatsächlich einen Verstoß gegen Art. 13 DS-GVO festgestellt hat, haben die Verantwortlichen regelmäßig selbst ihr Verfahren über die Information angepasst. Insgesamt waren Beschwerden zur Informationspflicht im Laufe des Jahres 2019 stark rückläufig. Das zeigt, dass die Verantwortlichen sich offenbar ihrer Pflicht zunehmend bewusst sind.

Mängel auf Webseiten

Ein weiterer großer Schwerpunkt betrifft den Bereich der Telemedien. Hier gingen zahlreiche Beschwerden ein, die sich mit

- unvollständigen Datenschutzerklärungen auf Webseiten,
- der Einbindung von Diensten wie Google Analytics oder Google Maps ohne notwendige Einwilligung,
- Veröffentlichungen von Fotos im Internet ohne Rechtsgrundlage (siehe dazu auch Kapitel J.10.3, S. 182),
- der nicht datenschutzkonformen Gestaltung von Formularen auf Webseiten sowie
- einer fehlenden oder unzureichenden Verschlüsselung von Webseiten (kein Einsatz von https://)

auseinander setzten.

Beschwerden gegen öffentliche Stellen

Schließlich erreichten mich auch zahlreiche Beschwerden, die den öffentlichen Bereich betrafen. Dabei ging es unter anderem um

- fehlende Rechtsgrundlagen für die Datenverarbeitung,
- die Offenlegung von Daten ohne Rechtsgrundlage oder Einwilligungen,
- nicht ausreichende Beauskunftungen gemäß § 51 NDSG durch eine Polizeibehörde,
- den Verdacht unrechtmäßiger Verarbeitungen durch die Polizei,
- den Verdacht unrechtmäßiger Videoüberwachung durch die öffentliche Hand,
- die unzulässige Speicherung von Inhalten der Führerscheinakte oder
- die Bearbeitung von Verkehrsordnungswidrigkeiten.

Wenige Bescheide angefochten

Gem. Art. 78 DS-GVO kann gegen Bescheide meines Hauses gerichtlich vorgegangen werden. Davon wurde im Berichtszeitraum aber nur selten Gebrauch gemacht, nämlich in insgesamt zwölf Fällen. Zum Teil richteten sich diese Klagen dagegen, dass mein Haus Beschwerden abgewiesen hatte. Andere Verfahren wurden angestrengt, da die von mir gewählte Abhilfebefugnis als rechtswidrig angesehen wurde. Zum Ende des Berichtszeitraums waren die Verfahren noch nicht abgeschlossen.

I.3. Datenpannen – Meldepflicht und typische Fallkonstellationen

Der für eine Datenverarbeitung Verantwortliche muss eine Vielzahl von Regelungen zum Schutz der verarbeiteten personenbezogenen Daten einhalten. Darüber hinaus müssen bestimmte Datenschutzverletzungen umgehend der Aufsichtsbehörde gemeldet werden. Diese Meldungen haben mit Geltung der Datenschutz-Grundverordnung (DS-GVO) in meiner Behörde immens zugenommen.

Rechtslage vor der DS-GVO

Schon das alte Datenschutzrecht kannte eine Pflicht zur Meldung bestimmter Datenschutzverstöße. Nach § 42a Bundesdatenschutzgesetz (BDSG) alter Fassung war diese Meldepflicht allerdings beschränkt auf besonders sensible Kategorien wie Gesundheitsdaten, Daten zu Straftaten oder Daten zu Bank- oder Kreditkartenkonten. Auch wurde die Meldepflicht nur durch eine unrechtmäßige Übermittlung oder sonstige unrechtmäßige Kenntnisnahme durch Dritte ausgelöst. Schließlich war sie an die Prognose gekoppelt, dass wegen der Kenntnisnahme durch Dritte schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen mussten. Die DS-GVO geht mit ihrer Regelung zur Meldepflicht bei Datenschutzverstößen nach Art. 33 deutlich weiter.

Voraussetzungen der neuen Meldepflicht

Jede Kategorie von Daten ist relevant

Jede Art einer Verletzung des Schutzes personenbezogener Daten löst die Meldepflicht gegenüber der Aufsichtsbehörde aus. Dies umfasst auch unbeabsichtigte Datenverluste oder Daten-Offenlegungen; ein Verschulden des Verantwortlichen ist nicht erforderlich, sogar zufällige Ereignisse können eine Datenschutzverletzung im Sinne des Art. 33 DS-GVO darstellen. Zudem ist nun jede Kategorie von betroffenen personenbezogenen Daten relevant – die Meldepflicht ist nicht wie früher auf bestimmte, besonders risikobehaftete Datenkategorien beschränkt.

Zusätzlich verpflichtet die DS-GVO nun auch Behörden zur Beachtung der Meldepflicht bei Datenschutzverletzungen. Gemeldet werden muss unverzüglich und möglichst innerhalb von 72 Stunden ab Kenntnis der Datenschutzverletzung.

Die Meldepflicht entfällt nur dann ausnahmsweise, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Anders als im früheren Recht besteht die

Pflicht damit nicht erst bei einer drohenden schwerwiegenden Beeinträchtigung der Rechte der Betroffenen. Besteht voraussichtlich sogar ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, muss der Verantwortliche die Betroffenen zusätzlich unverzüglich benachrichtigen.

Da es vollständig risikolose Verarbeitungen jedoch nicht geben kann, legt die Datenschutzkonferenz (DSK) die Formulierung „nicht zu einem Risiko" so aus, dass sie „nur zu einem geringen Risiko" führen darf. Sie hat sich auch in ihrem Erfahrungsbericht zur DS-GVO dafür ausgesprochen, die Meldepflicht nach Art. 33 DS-GVO auf Fälle zu beschränken, die voraussichtlich zu einem mehr als nur geringen Risiko für die Rechte und Freiheiten natürlicher Personen führen.

Risikoprognose

Der für die Datenverarbeitung Verantwortliche muss also bei einer Datenschutzverletzung zunächst das Risiko bewerten: Besteht überhaupt ein Risiko für die Rechte und Freiheiten natürlicher Personen bzw. sogar ein hohes? In der Praxis ist diese Bewertung mitunter schwierig. Da aber auch das Unterlassen einer verpflichtenden Meldung bußgeldbewehrt ist, melden Verantwortliche Datenschutzverletzungen teilweise vorsorglich, ohne selbst eine ausreichende Prüfung des Risikos durchgeführt zu haben.

Leitlinien für die Meldung von Datenschutzverletzungen: https://t1p.de/Leitlinien-zuArt33-Meldungen

Die Leitlinien aus dem Working Paper 250 der Art. 29-Datenschutzgruppe zur Meldung von Datenschutzverletzungen geben wertvolle Hinweise zur Bewertung des Risikos und nennen Beispiele für typische meldepflichtige Datenschutzverletzungen. Hierunter fallen etwa Cyberangriffe, bei denen personenbezogene Daten abgeschöpft oder offen ins Internet gestellt werden, oder die Versendung von Unterlagen an falsche Empfänger.

Pflichten des Auftragsverarbeiters

Wenn ein Auftragsverarbeiter eine Datenschutzverletzung im eigenen Tätigkeitsbereich feststellt, muss er diese unverzüglich an seinen Auftraggeber melden. Eine genau festgelegte Frist besteht dazu nicht. Der Auftraggeber muss die Datenschutzverletzung auch dann dem Verantwortlichen melden, wenn er selbst ein Risiko für die Rechte und Freiheiten natürlicher Personen für ausgeschlossen hält. Die Bewertung des Risikos obliegt allein dem Auftraggeber als Gesamtverantwortlichen für die Datenverarbeitung. Die Datenschutzverletzung gilt dem Verantwortlichen als „bekannt", sobald dieser von seinem Auftragsverarbeiter in Kenntnis gesetzt wurde (so die Leitlinien zur Meldung von Datenschutzverletzungen der Art. 29-Gruppe). Die Kenntnis des Auftragsverarbeiters wird also nicht dem Verantwortlichen zugerechnet.

Die DS-GVO nennt allerdings keine konkrete Frist, innerhalb der der Auftragsverarbeiter den Verantwortlichen informieren muss. Sie sieht nur vor, dass die Benachrichtigung „unverzüglich" zu erfolgen hat (Art. 33 Abs. 2 DS-GVO). Hier wird man im Regelfall eine sehr zeitnahe Meldung erwarten müssen. Deshalb empfehle ich, im Auftragsverarbeitungsvertrag organisatorische Maßnahmen vorzusehen, durch die der Verantwortliche die Meldung nach Art. 33 Abs. 2 DS-GVO so rechtzeitig erhält, dass er seinerseits die Meldung an die Aufsichtsbehörde innerhalb der 72-Stunden-Frist realisieren kann. Eine regelmäßige Höchstfrist von 72 Stunden besteht für den Auftrags-

verarbeiter jedenfalls nicht, schließlich könnte das im Extremfall zu einer Verdoppelung oder – bei Ketten-Auftragsverarbeitungsverträgen – zu einer weiteren Vervielfachung der Frist führen.

Bisweilen wird im Hinblick auf die europäische Fristenverordnung die Ansicht vertreten, die 72-Stunden-Frist müsste mindestens zwei volle Arbeitstage umfassen und könne sich entsprechend verlängern. Diese Auffassung teile ich nicht. Aufgrund der besonderen Dringlichkeit hat der Verordnungsgeber bewusst eine Stundenfrist vorgesehen, die etwa auch an einem Sonn- oder Feiertag enden kann und dementsprechend auch nicht durch das Erfordernis dazwischenliegender Arbeitstage verlängert wird. Überdies hat die Meldung im Ausgangspunkt „unverzüglich" zu erfolgen; auch das lässt keinen Raum für eine entsprechende Fristverlängerung.

Meldepflicht und Sanktionen

Das Unterlassen einer verpflichtenden Meldung nach Art. 33 DS-GVO ist bußgeldbewehrt (Art. 83 Abs. 4 lit. a DS-GVO). Die Meldung nach Art. 33 DS-GVO selbst darf allerdings gemäß § 43 Abs. 4 BDSG nicht in einem Ordnungswidrigkeitenverfahren wegen der Datenschutzverletzung verwendet werden. Eine Ausnahme gilt nur, wenn der Meldepflichtige selbst der Verwendung der Meldung in einem Bußgeldverfahren zustimmt. Diese Regelung ist Ausdruck des Grundsatzes der Selbstbelastungsfreiheit bzw. des Verbots der Selbstbezichtigung. Als Konsequenz darf die Aufsichtsbehörde die Informationen aus einer Meldung einer Datenschutzverletzung, welche zum Pflichtinhalt nach Art. 33 Abs. 3 DS-GVO gehören, nicht als Grundlage für ein Ordnungswidrigkeitenverfahren verwenden. Die Gegenansicht, die § 43 Abs. 4 BDSG für europarechtswidrig und damit für nicht anwendbar hält, überzeugt mich nicht.

Meldung darf nicht in Owi-Verfahren verwendet werden

Allerdings können Erkenntnisse über grundlegende Mängel aus einem weitergehenden Kontrollverfahren, das die Aufsichtsbehörde aufgrund der gemeldeten Datenschutzverletzung durchgeführt hat, verwendet werden. Stellt sich z. B. im Laufe eines aufgrund einer Meldung nach Art. 33 DS-GVO durchgeführten Prüfverfahrens heraus, dass grundlegende technisch-organisatorische Mängel beim Meldepflichtigen bestehen, können diese Gegenstand eines Bußgeldverfahrens sein. Denn die Selbstbelastungsfreiheit bezieht sich nur auf den konkret gemeldeten Datenschutzverstoß.

Durch die verschärfte Pflicht hat die Zahl der Datenschutzverletzungen, die meiner Behörde gemeldet werden, stark zugenommen. Im Jahr 2019 erreichten uns 824 Meldungen gemäß Art. 33 DS-GVO, davon mehr als 500 aus dem nicht-öffentlichen Bereich.

Mehr als 800 Meldungen im Jahr 2019

Infektion mit der Schad-Software Emotet

Neben anderen Fällen der Infektion mit Ransomware und Viren sowie diversen Hacking-Angriffen erreichten mich vielfach Meldungen, in denen es zu einem Befall mit der Schad-Software Emotet kam (siehe dazu auch Kapitel J.12.4, S. 195). Diese Angriffe führen dazu, dass dem Verantwortlichen der Zugriff auf die Daten durch Verschlüsselung entzogen wird. Aufgrund dieser Meldungen habe ich die Betroffenen auf den risikobasierten Ansatz der DS-GVO zu den datenschutzrechtlichen Anforderungen für alle Unternehmen hingewiesen, wie sie die Artikel 24, 25 und 32 der DS-GVO vorgeben. Diese enthalten die technisch-organisatorischen Rahmenbedingungen, inner-

halb derer „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen" vom Verantwortlichen geeignete, angemessene, zu dokumentierende und regelmäßig zu überprüfende Sicherheitsmaßnahmen zu treffen sind. Hierzu muss der Verantwortliche in einer eigenständig vorzunehmenden Risikobetrachtung geeignete technische und organisatorische Maßnahmen benennen, die dem ermittelten Risiko angemessen sind, und diese Maßnahmen auch umsetzen. Der Verantwortliche ist frei bei der Auswahl der Maßnahmen, solange das von ihm ermittelte Risiko damit angemessen berücksichtigt wird.

Verantwortlicher muss Risiken selbst prüfen

Zu Emotet veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits am 5. Dezember 2018 eine Pressemitteilung, in der es vor dieser Software warnte und Schutzmaßnahmen empfahl. Nach Maßgabe des BSI gäbe es zwar keine hundertprozentige Sicherheit, jedoch existierten verschiedene Schutzmaßnahmen, die sowohl auf organisatorischer als auch auf technischer Ebene umgesetzt werden könnten. Diese würden das Risiko einer Infektion mit Emotet oder auch anderer Schad-Software signifikant reduzieren.

Mitteilung des BSI: https://t1p.de/emotet

Häufig deckten sich die Angaben der von Emotet Betroffenen zu ihren vorab ergriffenen Maßnahmen nur teilweise mit den vom BSI veröffentlichten Schutzmaßnahmen. Zum Zeitpunkt der Meldung der Datenschutzverletzungen wurden mindestens eine, wenn nicht sogar mehrere der vom BSI veröffentlichten Schutzmaßnahmen, nicht beachtet.

Deshalb habe ich in diesen Fällen von meiner Abhilfebefugnis der Verwarnung nach Art. 58 Abs. 2 lit. b DS-GVO Gebrauch gemacht. Ich ging davon aus, dass die betroffenen Stellen künftig die vorbeugenden Schutzmaßnahmen gegen Emotet umsetzen würden. Im nicht-öffentlichen Bereich erklärte das Gros der betroffenen Unternehmen mir nachvollziehbar, ihre technischen und organisatorischen Maßnahmen für derartige Fälle angepasst zu haben.

SDM: https://t1p.de/sdm

Zur Einschätzung des risikobasierten Ansatzes empfahl ich das Kurzpapier Nr. 18: „Risiko für die Rechte und Freiheiten natürlicher Personen" der Datenschutzkonferenz (DSK). Ich verwies zudem zur methodischen Vorgehensweise auf das von der DSK bereitgestellte Standarddatenschutzmodell (SDM) und auf den in meinem Haus entwickelten „Prozess zur Auswahl angemessener Sicherungsmaßnahmen (ZAWAS)".

ZAWAS: https://t1p.de/zawas

Versand an einen falschen Empfänger

Mehrfach hatte ich sowohl im öffentlichen als auch im nicht-öffentlichen Bereich mit Meldungen von Datenschutzverletzungen nach Art. 33 DS-GVO zu tun, in denen personenbezogene Daten an einen unberechtigten Empfänger per Post oder E-Mail versendet wurden. Oftmals lag dabei die Ursache in technischem oder menschlichem Versagen. Die versendeten Schreiben enthielten häufig sensible personenbezogene Daten der Betroffenen gem. Art. 9 Abs. 1 DS-GVO.

Nach Art. 6 Abs. 1 S. 1 DS-GVO ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten nur unter den dort genannten Voraussetzungen zulässig. Nach Art. 5 Abs. 1 lit. f DS-GVO sind personenbezogene Daten so zu verarbeiten, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist. Da in Fällen des Fehlversands zum einen keine der

Integrität und Vertraulichkeit nicht mehr gegeben

Voraussetzungen des Art. 6 Abs. 1 S. 1 DS-GVO vorliegt und zum anderen durch die falsche Übermittlung die Integrität und Vertraulichkeit dieser Daten nach Art. 5 Abs. 1 lit. f DS-GVO auch nicht mehr gegeben ist, wurde gegen die datenschutzrechtlichen Bestimmungen verstoßen.

In derartigen Fällen habe ich ebenfalls von meiner Abhilfebefugnis der Verwarnung Gebrauch gemacht. Ich ging bezüglich des Postversands davon aus, dass dieser in künftigen Fällen datenschutzkonform erfolgen wird. Denn die Betroffenen erklärten in ihren jeweiligen Antwortschreiben nachvollziehbar, dass sie nach den Verstößen ihre Beschäftigten dazu angewiesen hatten, zukünftig sorgfältiger vorzugehen. Die datenschutzrechtliche Verfehlung beruhte auf individuellen Fehlern.

E-Mail-Verteiler: CC statt BCC

Bereits in meinem 22. Tätigkeitsbericht habe ich die Thematik der unzulässigen offenen Übermittlung von E-Mail-Adressen behandelt. Auch im Berichtszeitraum erreichten mich zahlreiche Art.-33-Meldungen von Unternehmen und öffentlichen Stellen, in denen es zu einem E-Mail-Versand per CC statt per BCC kam. Da in diesen Fällen ebenfalls keine der Voraussetzungen des Art. 6 Abs. 1 S. 1 DS-GVO vorliegt und zudem die Integrität und Vertraulichkeit dieser Daten nach Art. 5 Abs. 1 lit. f DS-GVO nicht mehr gegeben ist, wurde auch hier gegen datenschutzrechtliche Bestimmungen verstoßen.

22. Tätigkeitsbericht: https://t1p.de/tb2013-14

Auch in derartigen Fällen habe ich Verwarnungen ausgesprochen. Die Prüfung der bei mir eingegangen Meldungen zeigte, dass die Verantwortlichen grundsätzlich geeignete Verfahren implementiert haben, die eine Einhaltung der Betroffenenrechte gewährleisten. In ihren Schreiben schilderten mir zahlreiche Verantwortliche, ihr Personal angesichts solcher Vorfälle datenschutzrechtlich fortgebildet zu haben.

I.4. Bußgeldstelle
– Schwerpunkte und Berechnung von Geldbußen

Mit der Datenschutz-Grundverordnung (DS-GVO) wurde ein neuer Sanktionsrahmen festgelegt. Dieser sieht Bußgelder bis zu 20 Millionen Euro bzw. 4 Prozent des weltweiten Vorjahresumsatzes eines Unternehmens bei (eher) materiellen Verstößen und bis zu 10 Millionen Euro bzw. 2 Prozent des weltweiten Vorjahresumsatzes bei (eher) formellen Verstößen gegen die Verordnung vor. Es ist Aufgabe meiner Behörde, diesen Bußgeldrahmen angemessen und transparent anzuwenden.

Weitere wesentliche Neuerungen

Abschreckungseffekt erwünscht

Geldbußen müssen nach Art. 83 Abs. 1 DS-GVO wirksam, verhältnismäßig und zugleich auch abschreckend sein. Letzteres zielt nicht nur auf die mit dem Bußgeld belegten Unternehmen ab, sondern auch auf unbeteiligte Dritte, die davon abgehalten werden sollen, vergleichbare Verstöße zu begehen.

Geldbußen für Auftragsverarbeiter

Geldbußen können nach neuem Recht nicht mehr nur gegen Verantwortliche, sondern auch gegen Auftragsverarbeiter gerichtet sein. Damit wird dem Umstand Rechnung getragen, dass gerade kleinere Unternehmen sich häufig größerer Auftragsverarbeiter bedienen. Diese haben wiederum eine Marktmacht, welche die Aushandlung individueller Verträge erschwert oder gar unmöglich macht. Die mögliche Sanktionierung von Auftragsverarbeitern soll dazu beitragen, dass auch diese ein gesteigertes Interesse an der Rechtmäßigkeit der bei ihnen getätigten Datenverarbeitung haben.

Vor der DS-GVO wurde über sämtliche datenschutzrechtliche Ordnungswidrigkeitenverfahren vor den Amtsgerichten in öffentlicher Sitzung verhandelt. Nun werden Verfahren mit Geldbußen über 100.000 Euro vor den Landgerichten verhandelt.

Zurechnung zum Unternehmen

Adressaten von Bußgeldbescheiden nach dem Datenschutzrecht sind gemäß Art. 83 Abs. 3 DS-GVO die Verantwortlichen bzw. Auftragsverarbeiter. Nach der Definition in Art. 4 Nr. 7 DS-GVO kann dies eine natürliche oder juristische Person sein. Damit sind im Datenschutzrecht auch ohne Weiteres Geldbußen gegen Unternehmen möglich. Bei Unternehmensgruppen bzw. Konzernen wird bei Verstößen der funktionale Unternehmensbegriff angewendet[1]. Da-

Funktionaler Unternehmensbegriff

1 Der funktionale Unternehmensbegriff findet bereits in der ständigen EuGH-Rechtsprechung Anwendung, bislang allerdings noch nicht in Bezug auf das Datenschutzrecht.

nach wird ein Unternehmen definiert als jede wirtschaftliche Einheit unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung. Erwägungsgrund 150 der DS-GVO weist für die Verhängung von Geldbußen wegen Datenschutzverstößen gegen Unternehmen klarstellend auf den funktionalen Unternehmensbegriff hin.

Bislang ist die Anwendung des kartellrechtlich-funktionalen Unternehmensbegriffs noch strittig, wenngleich nicht auf Seiten der Datenschutzaufsichtsbehörden. Die europäischen Aufsichtsbehörden vertreten in den „Leitlinien für die Anwendung und Festsetzung von Geldbußen" (Working Paper 253) die Auffassung, dass dieser Unternehmensbegriff maßgeblich ist. Im Kurzpapier Nr. 2 zu Aufsichtsbefugnissen und Sanktionen hat sich die Datenschutzkonferenz ebenfalls auf diese Lesart verständigt.

Der Gesetzgeber hat mit § 41 Bundesdatenschutzgesetz (BDSG) die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) für sinngemäß anwendbar erklärt und lediglich einzelne Normen vom Anwendungsbereich herausgenommen. Weiterhin sind die §§ 30 und 130 OWiG, welche die Zurechnung von Handlungen Einzelner zum Unternehmen sowie den Tatbestand der Aufsichtspflichtverletzungen regeln, nicht anzuwenden, da sie mit den Regelungen der DS-GVO nicht in Einklang zu bringen sind[2].

Die Geldbuße kann auch dann gegenüber dem Unternehmen festgesetzt werden, wenn die Ordnungswidrigkeit nicht von einem vertretungsberechtigten Organ oder einer sonstigen für die Leitung verantwortlichen Person begangen wurde. Nach der ständigen Rechtsprechung des Europäischen Gerichtshofs haften Unternehmen auch für das Fehlverhalten ihrer Beschäftigten. Eine Kenntnis oder gar Anweisung der Geschäftsführung oder eine Verletzung der Aufsichtspflicht ist nicht erforderlich. Ausgenommen von dieser Zurechnung sind Exzesse von Beschäftigten. Diese liegen vor, wenn Handlungen der Beschäftigten bei verständiger Würdigung nicht mehr dem Kreis der jeweiligen unternehmerischen Tätigkeit zugeordnet werden können. Das ist zum Beispiel der Fall, wenn ein Mitarbeiter eine Kundendatenbank für private Zwecke missbraucht.

Thematische Schwerpunkte der Bußgeldstelle

Das Jahr 2019 war von der Entwicklung und Implementierung eines Bußgeldkonzeptes geprägt. Zudem wurden die vorhandenen Ermittlungsinstrumente in geeigneten Fällen intensiver genutzt. Insbesondere führte meine Behörde häufiger Beschlagnahmen durch und erwirkte häufiger Durchsuchungs- und Beschlagnahmeanordnungen beim zuständigen Gericht.

Durchsuchung und Beschlagnahme

Die überwiegende Zahl der Fälle im Jahr 2019 war dem Bereich der Videoüberwachung zuzuordnen. Neben einer größeren Zahl von Dashcam-Fällen (siehe dazu auch Seite 105) gab es einige Unternehmen, die ihre Kunden beobachteten sowie das Verhalten und die Leistung ihrer Beschäftigten überwachten. Einige dieser Fälle sind auch im Jahr 2020 noch anhängig.

2 Entschließung der 97. Konferenz der DSK am 3. April 2019: https://t1p.de/Haftung

Keine Geldbußen gegen Behörden möglich

In wenigen Fällen wurden Verfahren eingestellt, da es sich um (potenzielle) Verstöße einer Behörde gehandelt hat, die nicht als Exzess den handelnden Beschäftigten zuzurechnen waren. Die Behörden profitierten von der Privilegierung aus § 20 Abs. 5 NDSG. Aufgrund dieser Vorschrift bin ich grundsätzlich nicht befugt, Geldbußen gegenüber öffentlichen Stellen zu verhängen. Die Entscheidung des Gesetzgebers, auf diese Befugnisse zu verzichten, ist nicht nur bedauerlich. Sie hat zugleich meine Durchsetzungsmöglichkeiten gegenüber Behörden deutlich geschwächt, wenn nicht sogar verhindert. Verschiedenen anderen Aufsichtsbehörden in den EU-Mitgliedstaaten stehen solche Befugnisse zur Verfügung. So hat beispielsweise die norwegische Aufsichtsbehörde eine Geldbuße von etwa 170.000 Euro gegen die Stadt Bergen wegen erheblicher Verstöße gegen Art. 5 Abs. 1 lit. f und Art. 32 DS-GVO festgesetzt[3]. Der niedersächsische Gesetzgeber hat meiner Behörde diese wirksame Befugnis nicht zur Verfügung gestellt[4].

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

Zumessung von Geldbußen

Im Jahr 2019 hat sich nicht nur meine Behörde sehr intensiv mit der Frage auseinandergesetzt, wie Geldbußen bemessen werden können. Die Konferenz der unabhängigen Datenschutzbehörden von Bund und Ländern (DSK) hat ein gemeinsames Bußgeldkonzept entwickelt, das meine Behörde anwendet. Insgesamt habe ich 2019 aufgrund von Verstößen gegen die DS-GVO Geldbußen in Höhe von fast 480.000 Euro ausgesprochen. Zum Ende des Berichtszeitraums war aber der ganz überwiegende Teil dieser Summe noch nicht rechtskräftig.

Neben der Mitwirkung am Bußgeldkonzept der DSK stellte sich die komplexe Frage, inwieweit sich tat- und täterbezogene Umstände sowie das Verhalten des Betroffenen nach der Tat auf die Geldbuße auswirken. Für jedes Kriterium des Art. 83 Abs. 2 DS-GVO konnten typische Umstände identifiziert werden, welche sich mildernd oder erhöhend auf die zu erwartende Geldbuße auswirken.

A. Grundsätzliches Vorgehen (Konzept der DSK)

Die DSK hat im Oktober 2019 ihr Konzept zur Bußgeldzumessung in Verfahren gegen Unternehmen veröffentlicht. Dabei handelt es sich um ein „lernendes System". Veränderungen und Ergänzungen aufgrund von Rechtsprechung und neuen Erkenntnissen aus den europaweiten Abstimmungen sind in Zukunft möglich.

3 Quelle: https://www.datatilsynet.no/en/regulations-and-tools/reports-on-specific-subjects/administrative-fine-of-170.000--imposed-on-bergen-municipality/

4 24. Tätigkeitsbericht, S. 30, 31

Bei der Zumessung sind folgende fünf Schritte vorgesehen:

1. Kategorisierung nach Größenklassen

Unternehmen werden anhand ihres weltweiten Jahresumsatzes (in Euro) in eine von insgesamt 20 Größenklassen eingeteilt (Tabelle 1 des Konzeptes).

Kleinste Unternehmen		Kleine Unternehmen		Mittlere Unternehmen		Große Unternehmen	
A		B		C		D	
A.I	bis 700.000	B.I	bis 5 Mio.	C.I	bis 12,5 Mio.	D.I	bis 75 Mio.
A.II	bis 1,4 Mio.	B.II	bis 7,5 Mio.	C.II	bis 15 Mio.	D.II	bis 100 Mio.
A.III	bis 2,0 Mio.	B.III	bis 10 Mio.	C.III	bis 20 Mio.	D.III	bis 200 Mio.
				C.IV	bis 25 Mio.	D.IV	bis 300 Mio.
				C.V	bis 30 Mio.	D.V	bis 400 Mio.
				C.VI	bis 40 Mio.	D.VI	bis 500 Mio.
				C.VII	bis 50 Mio.	D.VII	über 500 Mio.

Beispiel: Ein Unternehmen mit einem weltweiten Jahresumsatz von 7 Millionen Euro würde nach dem Konzept in Stufe B.II eingeordnet, der Kategorie für über 5 bis 7,5 Millionen Euro weltweiten Jahresumsatz.

2. Bestimmung des mittleren Jahresumsatzes je Größenklasse

Anschließend wird der mittlere Jahresumsatz der Größenklasse in Euro bestimmt. Dazu werden jeweils der Anfangs- und Endbetrag der Klasse addiert und durch zwei dividiert.

Kleinste Unternehmen		Kleine Unternehmen		Mittlere Unternehmen		Große Unternehmen	
A		B		C		D	
A.I	350.000	B.I	3,5 Mio.	C.I	11,25 Mio.	D.I	62,5 Mio.
A.II	1,05 Mio.	B.II	6,25 Mio.	C.II	13,75 Mio.	D.II	87,5 Mio.
A.III	1,7 Mio.	B.III	8,75 Mio.	C.III	17,5 Mio.	D.III	150 Mio.
				C.IV	22,5 Mio.	D.IV	250 Mio.
Ab einem jährlichen Umsatz von 500 Mio. (D.VII) ist der prozentuale Bußgeldrahmen als Höchstgrenze zugrunde zu legen.				C.V	27,5 Mio.	D.V	350 Mio.
				C.VI	35 Mio.	D.VI	450 Mio.
				C.VII	45 Mio.	D.VII	Konkreter Jahres-umsatz

Im Fall von Klasse B.II liegt der mittlere Jahresumsatz der Kategorie bei 6,25 Millionen Euro (Tabelle 2).

3. Ermittlung des wirtschaftlichen Grundwertes

Berechnung eines Tagessatzes

Der mittlere Jahresumsatz wird herangezogen und durch 360 geteilt, sodass eine Art Tagessatz errechnet wird, der den wirtschaftlichen Grundwert in Euro abbildet.

Kleinste Unternehmen		Kleine Unternehmen		Mittlere Unternehmen		Große Unternehmen	
A		B		C		D	
A.I	972	B.I	9.722	C.I	31.250	D.I	173.611
A.II	2.917	B.II	17.361	C.II	38.194	D.II	243.056
A.III	4.722	B.III	24.306	C.III	48.611	D.III	416.667
				C.IV	62.500	D.IV	694.444
				C.V	76.389	D.V	972.222
				C.VI	97.222	D.VI	1.250.000
				C.VII	125.000	D.VII	Konkreter Tages-umsatz

Ab einem jährlichen Umsatz von 500 Mio. (D.VII) ist der prozentuale Bußgeldrahmen als Höchstgrenze zugrunde zu legen.

In Größenklasse B.II ergibt sich ein wirtschaftlicher Grundwert in Höhe von 17.361 Euro (Tabelle 3).

4. Multiplikation des Grundwertes nach Schweregrad der Tat

Anschließend werden die tatbezogenen Umstände aus Art. 83 Abs. 2 Satz 2 DS-GVO berücksichtigt, um zunächst den Schweregrad und anschließend den konkreten Faktor zu bestimmen. Es kommt jeweils eine vierstufige Skala zur Anwendung. Den Verstößen i.S.d. Art. 83 Abs. 4 DS-GVO (kleinerer Bußgeldrahmen bei (eher) formellen Verstößen) und Art. 83 Abs. 5, 6 DS-GVO (größerer Bußgeldrahmen bei eher (materiellen) Verstößen) werden jeweils unterschiedliche Faktoren zugeordnet.

Schweregrad der Tat	Faktor für (eher) formelle Verstöße gemäß Art. 83 Abs. 4 DS-GVO	Faktor für (eher) materielle Verstöße gemäß Art. 83 Abs. 5, 6 DS-GVO
Leicht	1 bis 2	1 bis 4
Mittel	2 bis 4	4 bis 8
Schwer	4 bis 6	8 bis 12
Sehr Schwer	≥ 6	≥ 12

Vier Schweregrade je „Verstoßkategorie"

Bei einem „mittleren" Verstoß im Bereich des größeren Bußgeldrahmens wäre ein Faktor von 4 bis 8 anwendbar, was bei Größenklasse B.II einen Korridor zwischen 69.444 und 138.888 Euro eröffnet. Um den konkreten Faktor festzulegen, werden in diesem Korridor die (weiteren) konkreten tatbezogenen Umstände berücksichtigt.

5. Anpassung anhand aller sonstigen Umstände

Anschließend wird das Bußgeld anhand aller für und gegen den Betroffenen sprechenden Umstände angepasst, soweit sie noch nicht in den vorherigen Schritten berücksichtigt wurden. Hierzu zählen insbesondere die täterbezogenen Umstände. Im Einzelfall kann der im vorherigen Schritt „eröffnete" Korridor nach oben oder unten verlassen werden.

B. Kriterien im Einzelnen

Das oben dargestellte Konzept erlaubt bereits eine Eingrenzung möglicher Geldbußen gegen Verantwortliche. Die vorhandenen Spannen sind jedoch noch immer relativ weit. Diese werden ausgefüllt, indem bei den Kriterien nach Art. 83 Abs. 2 DS-GVO die mildernden und erhöhenden Umstände berücksichtigt werden.

lit.	Mildernde Umstände	Erhöhende Umstände
a	Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens	
	• (sehr) kurze Dauer des Verstoßes • Art, Umfang oder Zweck der Verarbeitung sind datenschutzrechtlich wünschenswert • (sehr) wenige betroffene Personen • (sehr) geringer / kein erlittener Schaden	• (sehr) lange Dauer des Verstoßes • Art, Umfang oder Zweck der Verarbeitung sind datenschutzrechtlich zu missbilligen • (sehr) viele betroffene Personen • (sehr) schwerer erlittener Schaden
b	Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes	
	Leichte Fahrlässigkeit	Vorsatz / Absicht
c	jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens	
	Maßnahmen haben (weitere) Schäden ausgeschlossen	Notwendige Maßnahmen wurden nicht ergriffen
d	Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen	
	Geringe Verantwortlichkeit unter Berücksichtigung von Art. 25, 32 DS-GVO	(Sehr) Hohe Verantwortlichkeit unter Berücksichtigung von Art. 25, 32 DS-GVO
e	etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters	
	-	Ein oder mehrere einschlägige Verstöße
f	Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern	
	Die Zusammenarbeit mit der Aufsichtsbehörde hat das durch Art. 31 DS-GVO erwartete Niveau deutlich übertroffen	Keine / schlechte Zusammenarbeit mit der Behörde im vorherigen Verwaltungsverfahren

g	Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind	
	-	• Besondere Kategorien personenbezogener Daten • Andere besonders sensible Daten
h	Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat	
	Der Verantwortliche hat den Verstoß selbst gemeldet	Die Behörde wurde durch Beschwerde / Hinweis / Presse auf den Verstoß aufmerksam
i	Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurde	
	-	Nichteinhaltung der spezifischen Maßnahmen
j	Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42	
	Einhaltung genehmigter Verhaltenskodizes oder genehmigter Zertifizierungsmechanismen	Nichteinhaltung von genehmigten Verhaltenskodizes oder genehmigten Zertifizierungsmechanismen
k	jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste	
	• Wirtschaftliche Situation (z. B. drohende Insolvenz) • Geständnis • Lange Verfahrensdauer • Ernsthaft auf Vermeidung von Verstößen ausgelegtes Compliance-System	• Wirtschaftliche Situation (z. B. ungewöhnlich hohe Umsatzrentabilität) • Bedeutender wirtschaftlicher Vorteil im Zusammenhang mit dem Verstoß

Zu welchen Milderungen und Erhöhungen solche Umstände bei der Zumessung führen, ist vom Einzelfall abhängig. Eine Pauschalisierung sämtlicher Kriterien ist aufgrund der vielfältig möglichen Ausprägungsgrade nicht möglich.

I.5. Bußgeldverfahren gegen Dashcam-Einsatz

In der Vergangenheit haben Verantwortliche lediglich Verwarnungen und Hinweise bei der Nutzung von Dashcams erhalten. Seit dem Jahr 2019 setze ich nun grundsätzlich Bußgelder wegen des Gebrauchs der Kameras fest.

Der Einsatz von Dashcams nimmt auch in Niedersachsen immer mehr zu. Meistens soll bei einem Unfall der Hergang nachvollzogen und das Video als Nachweis für die Klärung von Haftungsfragen herangezogen werden. Typischerweise wird dazu das gesamte Umfeld aufgenommen; unbeteiligte Personen oder Kennzeichen anderer Fahrzeuge werden nicht verpixelt. Zugleich ist die Bildqualität bei einigen Kameras so gut, dass Personen und Kennzeichen selbst aus einiger Entfernung gut zu erkennen sind.

Fahrer wollen Haftungsfragen klären

Dashcam-Einsatz ist unzulässig

Wird mit Videoüberwachungsanlagen – einschließlich sog. Dashcams – in öffentlich zugänglichen Bereichen gefilmt, ist deren Einsatz an Art. 6 Abs. 1 Satz 1 lit. f der Datenschutz-Grundverordnung (DS-GVO) zu messen. Danach ist die Verarbeitung personenbezogener Daten nur zulässig, soweit dies zur Wahrung berechtigter Interessen von Verantwortlichen oder Dritten erforderlich ist. Zudem dürfen nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, die den Schutz personenbezogener Daten erfordern. Das bedeutet, die Interessen desjenigen, der eine Dashcam einsetzt, sind mit den Interessen der davon Betroffenen abzuwägen.

Entschließung der DSK zu Dashcams: https://t1p.de/dashcams

Wird das Verkehrsgeschehen permanent und anlasslos aufgezeichnet, überwiegen die schutzwürdigen Interessen betroffener Personen meist. Denn bei diesen handelt es sich überwiegend um unbeteiligte Verkehrsteilnehmer. Sie können sich insbesondere auf ihr Grundrecht aus Art. 8 der Charta der Grundrechte der Europäischen Union berufen. Danach hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dies umfasst das Recht des Einzelnen, sich in der Öffentlichkeit frei zu bewegen, ohne befürchten zu müssen, ungewollt und anlasslos zum Objekt einer Videoüberwachung gemacht zu werden.

Keine anlasslose Videoüberwachung

Dauerhaft aufzeichnende Dashcams erheben permanent und ohne Anlass personenbezogene Daten, wie Kennzeichen[1] der anderen Verkehrsteilnehmer

1 Kennzeichen sind personenbezogene Daten: OLG Celle, Beschl. v. 04.10.2017, 3 Ss (OWi) 163/17

sowie Personen, die sich in der Nähe einer Straße aufhalten. Es ist also eine Vielzahl von Verkehrsteilnehmern von der Verarbeitung betroffen, ohne dass sie von der Überwachung wissen oder sich dieser entziehen können. Das Interesse des Autofahrers als datenschutzrechtlich Verantwortlicher, nach einem Verkehrsunfall Videoaufnahmen als Beweismittel zu besitzen, kann diesen gravierenden Eingriff in das Recht auf Schutz der personenbezogenen Daten der anderen Verkehrsteilnehmer nicht rechtfertigen.

BGH-Entscheidung

Zudem muss auch bei einer Videoüberwachung mit Dashcam der Verantwortliche sicherstellen, dass er die betroffenen Personen gemäß Art. 12ff. DS-GVO auf die kameragestützte Verarbeitung personenbezogener Daten transparent hinweist. Gerade bei fahrenden Fahrzeugen wirft das in praktischer Hinsicht Schwierigkeiten auf.

Auch wenn der Bundesgerichtshof in seiner Entscheidung vom 15. Mai 2018[2] eine Beweisverwertbarkeit von Aufnahmen im Zivilprozess nicht verneint, betont er gleichzeitig, dass der anlasslose Einsatz von dauerhaft aufzeichnenden Dashcams datenschutzrechtlich unzulässig ist.

Im Ergebnis ist die Verwendung von Dashcams für die genannten Zwecke kaum zulässig möglich.

Behördliches Vorgehen

Zu Zeiten des Bundesdatenschutzgesetzes in alter Fassung habe ich lediglich in einem Extremfall ein Bußgeldverfahren durchgeführt.[3] Damals wurde durch das Amtsgericht Hannover eine Geldbuße festgesetzt, die vom Oberlandesgericht Celle bestätigt wurde. Das OLG bestätigte meine Auffassung, dass ein Fahrzeugkennzeichen als personenbezogenes Datum zu qualifizieren ist.

Um den Verantwortlichen die Rechtswidrigkeit der Dashcam-Nutzung vor Auge zu führen, ahnde ich den anlasslosen Betrieb mit permanenter Speicherung als Ordnungswidrigkeit. Als anlasslos gilt der Betrieb insbesondere, wenn die Kamera bei Fahrtantritt aktiviert wird und der Speicher erst überschrieben wird, sobald er vollläuft (rotierende Aufzeichnung).

Keine Sanktion bei anlassbezogenem Betrieb

Nicht sanktioniert wird der lediglich anlassbezogene Betrieb, auch wenn die Voraussetzungen des Art. 12ff. DS-GVO im Einzelfall nicht vorgelegen haben sollten. Anlassbezogen ist der Betrieb, wenn nur solche Sequenzen gespeichert werden, die in einem engen zeitlichen Zusammenhang mit einem auslösenden Ereignis stehen. Nimmt die Kamera dazu eine anlassloses Vorabaufzeichnung (Prerecording) von bis zu 30 Sekunden vor, besteht an der Verfolgung als Ordnungswidrigkeit meinerseits in der Regel kein besonderes Interesse und das Verfahren wird eingestellt.

Um eine gleichmäßige Herangehensweise zu fördern, habe ich für die Polizeidienststellen ein Merkblatt herausgegeben. Zugleich habe ich ein Informationsblatt erstellt, das Autofahrern von den Polizeibeamten ausgehändigt werden kann, wenn sie mit einer mutmaßlich unzulässig eingesetzten Dashcam angetroffen werden.

2 VI ZR 233/17

3 24. Tätigkeitsbericht, S. 153-155

Die im Jahr 2019 festgesetzten 9 Geldbußen bewegten sich in der Regel um einen Betrag von 500 Euro. Im Fall eines unterdurchschnittlichen Einkommens wurde die Geldbuße bis auf 350 Euro ermäßigt, in anderen Fällen auf bis zu 1000 Euro erhöht. Erhöht wird insbesondere, wenn das Einkommen besonders hoch ist, ein besonders langer Zeitraum aufgezeichnet wurde oder mehrere Kameras eingesetzt waren.

Bußgelder zwischen 350 und 1000 Euro

Geldbußen zwischen 350 und 1000 Euro erscheinen gerade noch ausreichend, um eine, wenn auch geringe, abschreckende Wirkung zu entfalten. Eine künftige Anpassung ist nicht auszuschließen, wenn eine stärker abschreckende Wirkung erforderlich werden sollte.

Sonderfall: Veröffentlichung von Aufzeichnungen

Eine Steigerung zur bloßen Aufzeichnung stellt die Veröffentlichung von Dashcam-Aufzeichnungen dar. Auf dem Internetportal YouTube finden sich eine Reihe von Kanälen, die geschnittene Dashcam-Aufzeichnungen der Allgemeinheit zugänglich machen, zum Teil ohne jede Verpixelung von Kennzeichen und Personen.

Einige dieser Videos haben die sog. Monetarisierungsfunktion aktiviert und verfügen über mehrere Millionen Aufrufe. Die Verantwortlichen verdienen mit dem Hochladen dieser Videos also Geld. In solchen Fällen sind Geldbußen im Bereich zwischen 350 und 1000 Euro nicht ausreichend. Zunächst muss der wirtschaftliche Vorteil berücksichtigt werden, so dass die Geldbußen auch fünfstellig ausfallen können. Ziel ist, dass der Betroffene keinen Vorteil durch seine rechtswidrige Handlung hat. Allerdings kann die Geldbuße nicht auf die bloße ‚Abschöpfung' dieses Vorteils begrenzt bleiben. Es ergäbe sich keine abschreckende Wirkung im Sinne des Art. 83 Abs. 1 DS-GVO, wenn lediglich die unter Missachtung des Datenschutzrechts generierten Einnahmen verloren gingen. Dann würde der Betroffene lediglich so gestellt, als hätte er den Verstoß nicht begangen. Insgesamt soll die Geldbuße daher die erzielten Einnahmen übersteigen.

Geldbußen müssen Einnahmen übersteigen

J. Aktuelle Themen

J.1. Polizei

1.1 Kritik zu polizeilichem Messenger-Dienst NIMes bleibt bestehen

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

Viele Beamtinnen und Beamte nutzen inzwischen den eigens für die Niedersächsische Polizei eingeführten Messenger NIMes. Bereits in meinem 24. Tätigkeitsbericht habe ich meine Bedenken dazu dargestellt. Eine eingehende technische Prüfung von NIMes war meiner Behörde auch im abgelaufenen Berichtszeitraum nicht möglich.

Der Pilotbetrieb für NIMes startete am 3. Mai 2018. Der eigene Messenger wurde eingeführt, um die interne Kommunikation der Polizei zu vereinfachen und die dienstliche Nutzung von kommerziellen Anbietern überflüssig zu machen. Diesen Aspekt begrüße ich sehr. Für mich ist es verständlich, dass die Polizei von den Vorteilen eines Messengers profitieren will. Schließlich stellt diese Art der Kommunikation eine enorme Zeitersparnis und eine allgemeine Erleichterung der Polizeiarbeit außerhalb der Dienststelle dar. Doch es gibt dabei einige zu beachtende Punkte

Problematisch ist zunächst die Ende-zu-Ende-Verschlüsselung. Grundsätzlich ist eine derartige Verschlüsselung in einer Anwendung, in der die Beamten der Polizei miteinander elektronisch kommunizieren, immer zu begrüßen. Sie unterbindet, dass unbefugte Personen die Kommunikation mitlesen können. In diesem Fall verhindert sie jedoch auch eine umfassende datenschutzrechtliche Kontrolle. Es ist den befugten Kontrolleuren ohne die Mitwirkung der Beamten nicht möglich, den erfolgten Austausch unter datenschutzrechtlichen Gesichtspunkten zu prüfen.

Unabhängig davon ist auch der Betrieb auf den privaten Mobiltelefonen der Beamten besonders kritisch, da er das Risiko von Sicherheitslücken erhöht.

Ende-zu-Ende-Verschlüsselung

Mit der Nutzungsvereinbarung von NIMes haben sich alle Anwender bereit erklärt, zur Kontrolle datenschutzrechtlicher Bestimmungen lesenden Zugriff auf die gesamten Kommunikationsinhalte zu gewähren. Während eines Evaluationszeitraums von Oktober 2018 bis Mai 2019 führte die Polizei anlassunabhängige Kontrollen durch. Erfreulicherweise wurden bei den Kontrollen keine Verstöße festgestellt. Auch auf anderem Weg, wie etwa im Rahmen einer Datenpannenmeldung gemäß § 41 NDSG, wurde mir kein datenschutzrechtliches Fehlverhalten bekannt.

Allerdings sind die datenschutzrechtlichen Kontrollen erheblich auszuweiten. Erst dann kann meine Behörde eine endgültige Bewertung vornehmen.

Sollte der freiwilligen anlassunabhängigen Kontrolle weiterhin in allen Fällen Folge geleistet werden, könnte eine effektive Kontrolle trotz Ende-zu-Ende-Verschlüsselung gewährleistet werden. Im Übrigen müssten – für den Fall der Verweigerung – dienstrechtliche Konsequenzen für den einzelnen Beschäftigten gezogen werden.

Nutzung privater Endgeräte

Bislang hatte ich noch keine Möglichkeit, die von der Polizei eingerichteten technischen Schutzmaßnahmen im Detail zu prüfen. Deshalb muss ich an der Forderung festhalten, dass NIMes nur auf dienstlichen Mobiltelefonen eingesetzt wird, um die Gefahr von Sicherheitslücken zu verringern. Sollte eine nachfolgende Prüfung jedoch ergeben, dass entsprechende Schutzmaßnahmen im vollen Umfang auf den privaten Endgeräten implementiert worden sind, halte ich ein Abrücken von meiner grundsätzlichen Ablehnung privater Endgeräte für denkbar.

Datenschutz-Folgenabschätzung fehlt

Zudem liegt mir keine Datenschutz-Folgenabschätzung (DSFA) zu NIMes vor. Diese ist unter anderem wegen des Umfangs und der Sensibilität der verarbeiteten Daten gesetzlich vorgeschrieben. Ich habe der Polizei empfohlen, eine DSFA nach dem Prozess zur Auswahl angemessener Sicherungsmaßnahmen „ZAWAS“ durchzuführen. Damit wird eine abschließende datenschutzrechtliche Bewertung der technisch-organisatorischen Schutzmaßnahmen ermöglicht. Das zu meiner Behörde gehörende Datenschutzinstitut Niedersachsen bietet entsprechende Schulungen zu ZAWAS an. Auf mein Angebot haben im Dezember 2019 zahlreiche Beschäftigte der Polizei Niedersachsen an dieser Schulung teilgenommen.

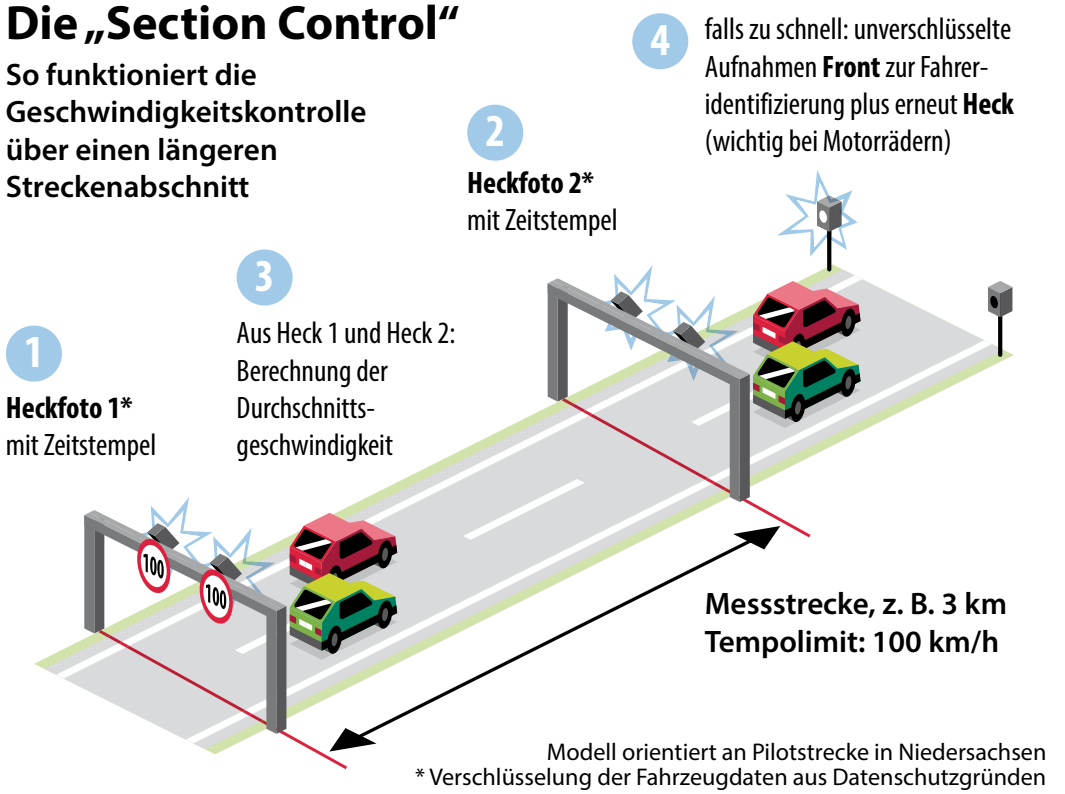
Mehr zu ZAWAS:
https://t1p.de/ZAWAS

Die Polizei ist nun aufgefordert, für NIMes eine DSFA zum aktuellen Stand vorzulegen. Erst danach kann meine Behörde die technischen Abläufe des Messengers überprüfen.

1.2 Abschnittskontrolle nun mit nötiger Rechtsgrundlage

Anfang 2019 ging die „Section Control" genannte Anlage zur Abschnittskontrolle auf der B 6 in Betrieb. Angesichts einer Entscheidung des Bundesverfassungsgerichts forderte ich aber nur wenig später, die Anlage wieder stillzulegen, bis eine spezifische Rechtsgrundlage für ihren Betrieb geschaffen war.

Die Entscheidung des Bundesverfassungsgerichtes (BVerfG) zur Frage des Grundrechtseingriffs von Nichttrefferfällen beim Einsatz von Kennzeichenlesegeräten kam einer Kehrtwende gleich. Sie führte unmittelbar dazu, dass die Rechtmäßigkeit der Abschnittskontrolle neu bewertet werden musste. Die frühere Rechtsprechung des BVerfG aus dem Jahr 2008[1] sagte aus, dass nur bei Trefferfällen ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vorläge.



1 BVerfG, 1 BvR 2075/05 und 1 BvR 1254/07

BVerfG: Auch Nichttreffer greifen in Grundrechte ein

Mit den Beschlüssen aus dem Dezember 2018[2] stufte das Gericht jedoch auch die kurzzeitige Erfassung der sogenannten Nichttreffer als Grundrechtseingriff ein. Von einem Eingriff waren also nicht nur die Autofahrer betroffen, die auf der B6 die Geschwindigkeit überschritten und „geblitzt" wurden, sondern alle, die diesen Abschnitt befuhren – das entspricht rund 15.000 Fahrzeugdatensätzen pro Tag. Damit war eine spezielle Rechtsvorschrift für die Abschnittskontrolle unabdingbar geworden.

Zunächst Zustimmung zum Pilotbetrieb

Tätigkeitsbericht 2015/16: https://t1p.de/tb2015-2016

Rückblick: Mit Erlass vom 12. Dezember 2014 hatte das Niedersächsische Ministerium für Inneres und Sport die „Section Control" zur Geschwindigkeitsüberwachung eines rund zwei Kilometer langen Streckenabschnitts auf der B6 einrichten lassen. Am 14. Januar 2019 hatte der Pilotbetrieb begonnen, geplant für 18 Monate. Diesem Pilotbetrieb hatte mein Vorgänger auf Grundlage der alten Rechtsprechung des BVerfG zugestimmt. Allerdings wurde schon damals deutlich gemacht, dass kein dauerhafter Einsatz ohne ausdrückliche Rechtsgrundlage möglich sei.

Angesichts der aktuellen Beschlüsse des BVerfG forderte ich nach Erhalt und Auswertung der Datenschutz-Folgenabschätzung das Niedersächsische Innenministerium am 6. Februar 2019 dazu auf, den Pilotbetrieb sofort zu beenden. In gleicher Weise äußerte sich meine Behörde in einer Anhörung des Innenausschusses am 7. Februar. Zudem erhob am 18. Februar 2019 ein betroffener Bürger Klage gegen die Polizeidirektion Hannover wegen des Betriebs der Abschnittskontrolle. Meine Behörde nahm als Beigeladene an dem Verfahren teil. Die Klage wurde unter anderem mit der fehlenden Rechtsgrundlage für den Betrieb begründet. Die Polizeidirektion wurde im einstweiligen Rechtsschutzverfahren und in der Hauptsache vom Verwaltungsgericht (VG) Hannover verurteilt, den Pilotbetrieb und den darüberhinausgehenden Einsatz des Geschwindigkeitsmessgerätes „Section Control" einzustellen. Der mit dem Betrieb verbundene Eingriff in die Persönlichkeitsrechte könne sich auf keine Rechtsgrundlage stützen.

VG Hannover ordnet Stilllegung an

Damit machte das VG Hannover deutlich, wie wichtig das Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts ist. Diese Ansicht wurde auch im Rahmen des durch die Polizeidirektion Hannover geführten Beschwerdeverfahrens im einstweiligen Rechtsschutz durch das Niedersächsische Oberverwaltungsgerichts (OVG) in Lüneburg bestätigt.

Notwendige Rechtsgrundlage im neuen Polizeigesetz

Bereits im verwaltungsgerichtlichen Verfahren teilte die Polizeidirektion mit, dass in wenigen Monaten mit einer spezifischen Rechtsgrundlage im Gesetzentwurf zur Novelle des Niedersächsischen Polizeigesetzes zu rechnen sei. Im Mai 2019 trat das Niedersächsische Polizei- und Ordnungsbehördengesetz (NPOG) dann in Kraft. Wie angekündigt, verfügte es nun mit § 32 Absatz 6 NPOG über eine spezifische Rechtsgrundlage für die Abschnittskontrolle.

OVG ändert Entscheidung

Das OVG Lüneburg änderte daraufhin auf Antrag der Polizeidirektion Hannover die im einstweiligen Rechtsschutz getroffene Entscheidung im Rahmen eines Verfahrens nach § 80 Absatz 7 der

2 BVerfG, 1 BvR 142/15, 1 BvR 2795/09 und 1 BvR 3187/10

Verwaltungsgerichtsordnung. Zudem fand am 13. November 2019 im Berufungsverfahren die mündliche Hauptverhandlung statt. Auch in dem darauf ergangenen Urteil änderte das OVG Lüneburg die Entscheidung des VG Hannover im Sinne der Polizeidirektion Hannover. Als Begründung wurde – wie von mir erwartet – angegeben, dass die betreffende Norm des NPOG rechtskonform beschlossen worden sei. Damit ist eine bereichsspezifische Rechtsgrundlage – wie von mir gefordert – für den dauerhaften Betrieb der Abschnittskontrolle gegeben.

Das OVG Lüneburg hat gegen seine Entscheidung keine Revision zugelassen. Dagegen hat der betroffene Bürger Nichtzulassungsbeschwerde eingelegt. Das verwaltungsgerichtliche Verfahren ist damit noch nicht abgeschlossen. Unabhängig davon wurde die Abschnittskontrolle Mitte November 2019 wieder in Betrieb genommen.

Weitere datenschutzrechtliche Vorgaben erfüllt

Darüber hinaus kam die Polizeidirektion Hannover meiner Aufforderung nach, auch die datenschutzrechtlichen Transparenz- und Informationspflichten beim Betrieb der Abschnittskontrolle zu erfüllen. Die entsprechenden Angaben sind prominent auf der Internetseite der Polizeidirektion Hannover eingebunden. Die Betroffenenrechte sind damit in ausreichender Weise gewahrt.

1.3 Leitstellen erfüllen gesetzliche Vorgaben nicht

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

In meinem 24. Tätigkeitsbericht hatte ich über die Verarbeitung hochsensibler Daten in den kooperativen bzw. eigenständigen Leitstellen der Polizei berichtet. Die unsachgemäße Handhabung der Daten kann Gesundheit, Freiheit oder sogar das Leben der Betroffenen beeinträchtigen.

Ich hatte in meinem vorherigen Bericht insbesondere bemängelt, dass die Polizeidirektion (PD) Oldenburg ihrem Auftrag, eine Muster-Datenschutz-Folgenabschätzung (Muster-DSFA) für die Leitstellen zu erstellen, an denen sich die Landespolizei beteiligt, auch nach mehr als sieben Jahren noch nicht abschließend nachgekommen ist. Meine mehrfachen Rügen gegenüber dem Innenministerium haben 2018 zu einer neuen Anordnung des Landespolizeipräsidiums geführt, in welcher die Polizeidirektion PD Oldenburg aufgefordert wurde, diese Muster-DSFA bis Ende 2019 vorzulegen.

Nach Auskunft der PD Oldenburg wurde dieses Dokument auch Anfang Dezember 2019 an das Innenministerium übersandt. Leider wurde mir die DSFA bis Redaktionsschluss dieses Berichts nicht zur Verfügung gestellt. Somit bin ich weiterhin nicht in der Lage, mich von den getroffenen technisch-organisatorischen Maßnahmen zum Schutz der verarbeiteten hochsensiblen Daten überzeugen zu können. Auf Nachfrage bestätigte mir das Innenministerium den fristgerechten Eingang der Muster-DSFA und stellte in Aussicht, dass ich die Dokumente bis Ende Februar 2020 zur Prüfung erhalte. Ich bestehe darauf, dass dieser zugesicherte Termin eingehalten wird.

Muster-DSFA soll bis Ende Februar 2020 vorliegen

Neue DSFA erforderlich

Zwischenzeitlich habe ich erfahren, dass im August 2019 einem neuen IT-Dienstleister der Zuschlag für die Implementierung einer neuen Leitstellentechnik und -software erteilt worden ist. Diese Technik und -Software wird zeitnah in allen Leistellen mit polizeilicher Beteiligung eingeführt. Damit einher geht die gesetzliche Verpflichtung, eine neue DSFA zu erstellen. Ich werde in diesem Fall fordern, mir eine entsprechende Abschätzung vor Inbetriebnahme der neuen Technik und Software vorzulegen.

Vertrag zur Auftragsverarbeitung fehlt

In nahezu allen Leitstellen wird die Einsatzleit-Software durch beauftragte IT-Unternehmen gewartet und betreut. Dabei werden auch Fernwartungszugriffe geschaltet, die im Zweifelsfall einen „Durchgriff“ auf die enthaltenen personenbezogenen Daten ermöglichen. Ich hatte bereits in der Vergangenheit festgestellt, dass diese Tätigkeiten in einigen Leitstellen nicht ausreichend

Fernwartung macht Vertrag zur Auftragsverarbeitung nötig

mit datenschutzrechtlichen Verträgen zur Auftragsverarbeitung abgesichert wurden. Diesen rechtswidrigen Zustand habe ich in der Vergangenheit ebenfalls gegenüber dem Innenministerium gerügt. Auch zu diesem Thema hat das Innenministerium im Jahr 2018 die Polizeibehörden aufgefordert, notwendige Verträge zeitnah abzuschließen und mir vorzulegen.

Bis auf eine PD haben mir zwischenzeitlich alle Polizeibehörden die erforderlichen Verträge zur Prüfung übersandt. Ich habe die ausstehende PD nun aufgefordert, mir einen endgültigen Termin zu nennen, wann der Vertrag mit dem Auftragnehmer geschlossen wird und für den Fall der Nichteinhaltung des Termins eine Beanstandung angekündigt.

1.4 Prüfungen zur Videoüberwachung in Fußballstadien

Bereits 2016 habe ich damit begonnen, die Videobeobachtung in niedersächsischen Fußballstadien umfassend zu prüfen. Kontrolliert wurden und werden Vereine, die in der Bundesliga, der 2. Bundesliga oder der 3. Liga spielen. Von ihnen verlangen die Richtlinien des Deutschen Fußballbundes (DFB) eine Videoüberwachung in den Stadien. Andernfalls drohen Konventionalstrafen. In Niedersachsen haben alle Vereine, die in den genannten Ligen spielen, eine Videoüberwachung eingerichtet.

Zwecke: Sicherheit der Besucher und Hausrecht

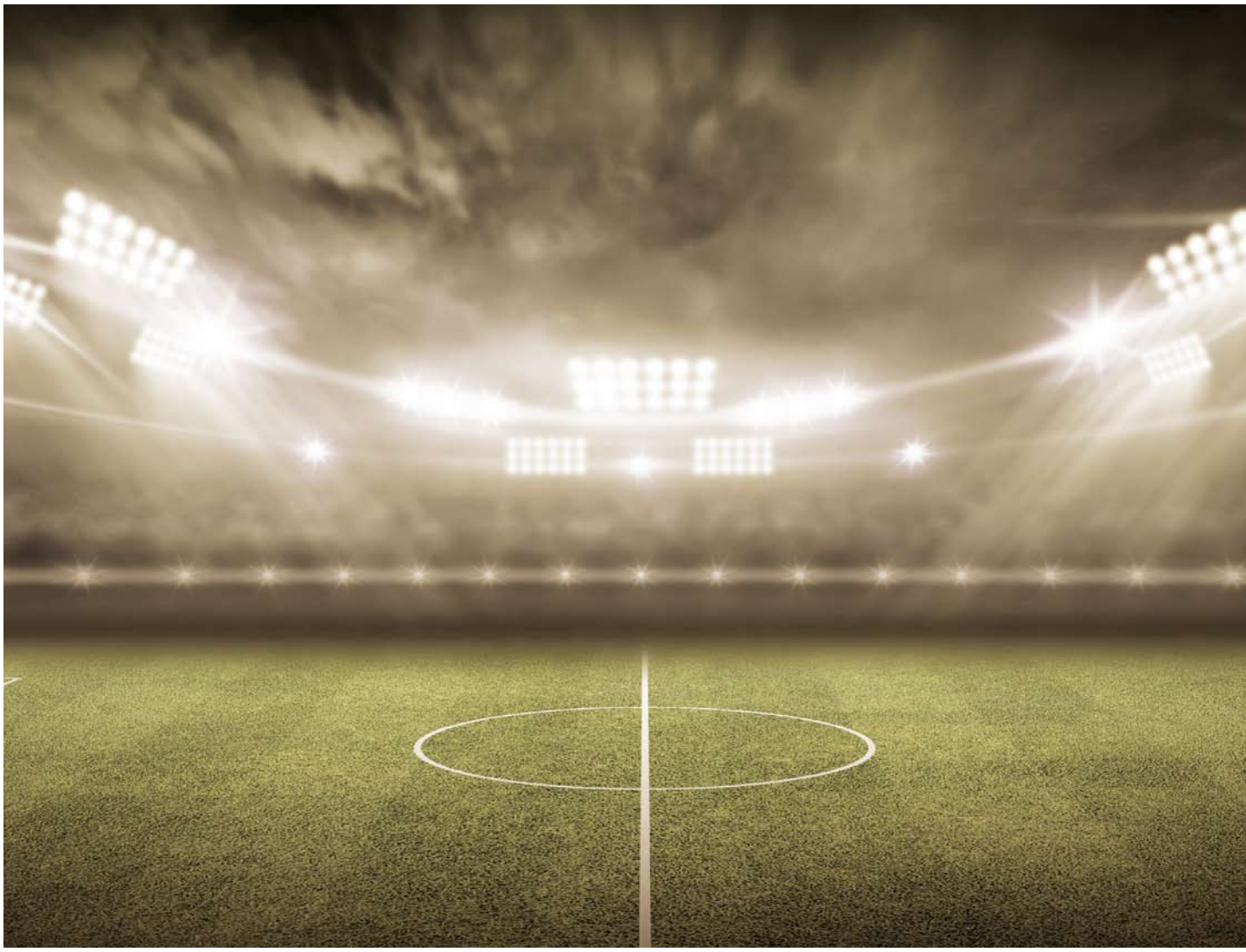
Die Videoüberwachung wird in allen Stadien während der Fußballspiele und anderer (Groß-)Veranstaltungen genutzt, um die Sicherheit der Besucher zu gewährleisten. Zudem wird teilweise auch außerhalb des Spielbetriebs und Veranstaltungen die Überwachung fortgesetzt, um das Hausrecht wahrnehmen zu können. Die Beobachtung findet grundsätzlich durch die Polizei statt, die ihr Vorgehen auf den § 32 Absatz 3 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG) stützt. Außerhalb der Spielzeiten oder von Veranstaltungen können die Vereine ihre Stadien auf Basis von Artikel 6 Absatz 1 Buchstabe f Datenschutz-Grundverordnung (DS-GVO) überwachen.

Ein Verein mauert – und wird kontrolliert

Ein Verein wurde erstmals 2016 und anschließend mehrfach von meiner Behörde beraten und gebeten, mit der Polizei Verträge zur datenschutzgerechten Ausgestaltung der Videobeobachtung abzuschließen. Da der Verein keine weiteren Bemühungen erkennen ließ, führte ich im Herbst 2019 eine unangekündigte Prüfung der Videobeobachtung an einem Spieltag durch.

Aufnahmen zu lang gespeichert

Im Rahmen dieser Kontrolle stellten wir unrechtmäßige Verarbeitungen fest. So wurden anlasslose Videoaufnahmen über einen Zeitraum von vier Wochen (statt zulässigen 72 Stunden) gespeichert. Auch war der Zugang zu den Servern, auf denen die Aufnahmen gespeichert waren, nicht nachvollziehbar und aus unserer Sicht unkontrolliert. Zudem nutzte der Verein im Spielbetrieb die Videobeobachtung auch für seine eigenen Sicherheitskräfte. Dies war jedoch für die vorgegebenen Zwecke nicht in allen Fällen geeignet und auch nicht erforderlich. Auf mein Drängen begann der Verein sofort mit einer Nachbesserung. Mittlerweile sind die wesentlichen Mängel behoben. Der Abschluss dieser Prüfung ist zeitnah zu erwarten.



Wie ist die Situation in anderen Stadien?

Bisherige Prüfungen in anderen Stadien haben gezeigt, dass die Videobeobachtung dort nur während des Spielbetriebs oder anderer Veranstaltungen in alleiniger Verantwortung der Polizei durchgeführt wird. Damit wird ein datenschutzgerechtes Vorgehen einfacher ermöglicht. Entsprechende Verträge zwischen dem Betreiber und der Polizei lagen vor. An diese halten sich nach meiner Erkenntnis alle Beteiligten. In den anderen geprüften Stadien sind zudem keine technisch-organisatorischen Mängel zur Speicherdauer und zu den Servern festgestellt worden.

Zwei weitere Prüfungen in 2020

In zwei weiteren Fußballstadien steht eine Überprüfung noch aus. Ich beabsichtige, diese im Jahr 2020 durchzuführen und damit die Prüfung insgesamt abzuschließen.

1.5 Aktendiebstahl im Landeskriminalamt

Durch Medienberichte wurde ich auf den Verlust personenbezogener Daten im Landeskriminalamt (LKA) aufmerksam. Grund war der Diebstahl einer Aktentasche aus dem Auto eines LKA-Beschäftigten. Dieser Vorgang stellte eine Verletzung des Schutzes personenbezogener Daten und damit ein meldepflichtiges Ereignis gemäß § 41 Absatz 1 des Niedersächsischen Datenschutzgesetzes (NDSG) in Verbindung mit Art. 33 Datenschutz-Grundverordnung (DS-GVO) dar.

Der Fall war besonders brisant, weil der in der Akte genannte Betroffene eine sogenannte Vertrauensperson war, deren Identität und Zusammenarbeit mit der Polizei gegenüber dritten Personen einer besonderen Geheimhaltung unterliegt. Trotz der Meldepflicht wurde mir die Datenpanne nicht – wie in § 41 Absatz 1 NDSG in Verbindung mit Art. 33 DS-GVO vorgeschrieben – gemeldet. Ich musste selbst die Initiative ergreifen und das LKA zu einer Stellungnahme auffordern. Fälschlicherweise ging das LKA davon aus, dass eine Meldung entbehrlich war. Das LKA verneinte ein Risiko für die Rechte der Vertrauensperson, da keine Einsichtnahme durch einen Unbefugten nachzuweisen war, nachdem die Behörde die Akten zurückerhalten hatte.

Informationen zur Meldung von Datenschutzverstößen: https://t1p.de/faq33

Noch keine abschließende Bewertung möglich

Im Rahmen der ersten Kontaktaufnahme unterrichtete ich das LKA über dessen datenschutzrechtliche Pflichten. Zusätzlich übersandte ich Fragen, um den Sachverhalt zu ermitteln und damit eine datenschutzrechtliche Prüfung zu ermöglichen.

Das LKA bot mir ein Erörterungsgespräch sowie Einsichtnahme in die relevante Dokumentation an. Dieses Angebot werde ich nach Abschluss der strafrechtlichen Ermittlungen annehmen. Erst dann wird eine abschließende datenschutzrechtliche Prüfung möglich sein.

Meldung von Datenpannen auch für öffentliche Stellen Pflicht

Ich nehme diesen Fall zum Anlass, um auf die folgenden gesetzlichen Regelungen hinzuweisen: Für die vom Anwendungsbereich des § 23 NDSG umfassten öffentlichen Stellen besteht seit dem 25. Mai 2018 nach § 41 des NDSG die Pflicht, meiner Behörde Datenpannen zu melden. Für die anderen öffentlichen Stellen ergibt sich die entsprechende Meldepflicht grundsätzlich unmittelbar aus Artikel 33 der DS-GVO.

Vielen Behörden scheint diese gesetzliche Verpflichtung nicht geläufig zu sein. Ich rate daher dringend allen Verantwortlichen, sich mit den Anforderungen der DS-GVO vertraut zu machen und diese umzusetzen.

1.6 Zentrum zur Telekommunikationsüberwachung – Projekt auf der Zielgeraden?

Die Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein errichten in Kooperation ein gemeinsames „Rechen- und Dienstleistungszentrum Telekommunikationsüberwachung der Polizei im Verbund der norddeutschen Küstenländer" (RDZ-TKÜ). Die Planungen hierzu wurden bereits im Jahr 2011 aufgenommen. Ziel des im August 2016 hierfür in Kraft getretenen Staatsvertrages ist eine neu zu konzipierende und von allen Stellen gemeinschaftlich genutzte TKÜ-Anlage.

Über die rechtlichen und technisch-organisatorischen Themen, die meine Behörde gemeinsam mit den anderen betroffenen Aufsichtsbehörden zu diesem Projekt behandelt hat, habe ich in den zurückliegenden vier Tätigkeitsberichten ausführlich berichtet. Dabei spielten auch die Lehren aus der noch immer nicht vollständig abgearbeiteten datenschutzrechtlichen Mängelliste der TKÜ-Anlage eine maßgebliche Rolle, die in Niedersachsen aktuell noch im Einsatz ist und bis zur Inbetriebnahme des neuen Verfahrens auch weiterhin im Einsatz sein wird.

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

Verzögerungen machen neue Prüfungen nötig

Nach der bisherigen Planung war als neuer Standort des Rechenzentrums der Neubau des Landeskriminalamts Niedersachsen in Hannover vorgesehen. Da sich das Neubauprojekt aus Haushaltsgründen verzögerte, musste die Polizei Überlegungen zu alternativen Standorten anstellen. Zudem wurde eine neue Projektleitung seitens der Polizei eingesetzt, mit der in Gesprächen der Planungsstand und die Datenschutzanforderungen zu besprechen waren.

Aus der Wahl des neuen Betriebsstandortes für das RDZ ergaben sich maßgebliche Änderungen der technischen und organisatorischen Rahmenbedingungen. Dies führte zu weiteren Verzögerungen in der Planung und zu weiterem Beratungsbedarf, dem die fünf beteiligten Datenschutzaufsichtsbehörden nachkamen. Teile der Leistungsbeschreibungen mussten angepasst werden. Zudem war es erforderlich, die damit verbundenen datenschutzrechtlichen Zulässigkeitsprüfungen unter maßgeblich geänderten Gesichtspunkten neu durchzuführen. Die sehr eng gesetzten Terminkorridore sowie die nur im Entwurfsstadium und in Detailfragen noch unvollständig und fragmentiert vorgelegten Dokumente machten eine eingehende Prüfung unmöglich.

Zusätzlich zur bisher zugrunde zu legenden Rechtslage kam, dass die Umsetzung der sogenannten JI-Richtlinie[1] in nationales Recht neu zu bewerten war, die sich in Niedersachsen in Teilen des neuen Niedersächsischen Datenschutzgesetzes (NDSG) wiederfindet. Daneben sind gleichberechtigt die zum Teil unterschiedlichen Bestimmungen der Landesdatenschutzgesetze der anderen Länder zu berücksichtigen.

Forderungen der Aufsichtsbehörden

Im Jahr 2019 gaben die Datenschutzaufsichtsbehörden der fünf Länder zwei gemeinsame Stellungnahmen ab, die sich zu zahlreichen Details der datenschutzrechtlichen und technisch-organisatorischen Maßnahmen einließen. Darin waren unter anderem folgende Gesichtspunkte von besonderer Bedeutung:

Folgenabschätzung muss vor Aufnahme des Betriebs vorliegen

- 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, Risikobewertung/Schutzbedarfsfeststellung und angemessenen Risikominimierung 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 und Dienststellen- und Organisationsebenen als Mandanten sichergestellt werden;

1 RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

- 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;
- Antiviren- und Backup-Lösungen sind auszugestalten.

Um Missverständnisse zu vermeiden, wurde verdeutlicht, dass die Datenschutzbeauftragten der Länder das Projekt RDZ-TKÜ beratend und nicht im Status einer Kontrolle begleiten, solange sich das Verfahren noch nicht im Echtbetrieb befindet. So wurden zu den vorgelegten Unterlagen Einschätzungen mitgeteilt und Hinweise für eine datenschutzkonforme Gestaltung des Verfahrens gegeben. Nicht damit verbunden war eine Zustimmung, Abnahme, Freigabe oder abschließende Beurteilung, die nach den jeweiligen Landesdatenschutzgesetzen auch nicht zu den Aufgaben der Landesbeauftragten gehören.

Beratung, keine Abnahme

Start verschiebt sich weiter

Im September 2019 wurde die Ausschreibung beendet und der Zuschlag erteilt. Die Aufsichtsbehörden wurden allerdings erst wesentlich später darüber informiert, welches Unternehmen den Zuschlag erhalten hatte, sodass sich eine Bewertung der nun konkret angebotenen Lösungen weiter verzögerte. Laut Staatsvertrag sollte der Wirkbetrieb mit Beginn des Jahres 2020 aufgenommen werden. Dieser Starttermin wird sich durch die Ausschreibung und den Standortwechsel sowie zusätzliche Wechselwirkungen erheblich verzögern.

Um Versäumnisse und aufwändige Nachbesserungen zu vermeiden, muss nach der Auswahl des Anbieters und seiner Software-Lösung in dem daraus resultierenden Gesamtverfahren nicht nur die Umsetzung der funktionalen Anforderungen optimiert werden. Außerdem muss mithilfe einer methodisch sauberen, vollständigen, nachvollziehbaren und pflegbaren Datenschutz-Folgenabschätzung auch allen rechtlichen und technisch-organisatorischen Bestimmungen entsprochen werden.

Ein solcher Prozess muss konsequent und ohne Abstriche beim Erfüllungsgrad der final festgelegten datenschutzrechtlichen Anforderungen umgesetzt werden. Andernfalls wären die TKÜ-Maßnahmen mit ihrer umfangreichen Eingriffstiefe in die Rechte und Freiheiten für die Betroffenen gesellschaftlich nicht tragbar und rechtlich unzulässig.

Auf einer für Ende Januar 2020 anberaumten Informationsveranstaltung berichtete die Projektgruppe RDZ-TKÜ über den aktuellen Sachstand und die weitere Vorgehensweise. Ich werde das Thema in meinem nächsten Tätigkeitsbericht wieder aufgreifen.

1.7 Fehlerhafte Speicherung führt zu jahrelangem Rechtsstreit

Ermittlungen der Polizei führten im Fall W. zu Speicherungen von fehlerhaften personenbezogenen Daten. Es dauerte lange, bis die Rechte der betroffenen Person umgesetzt werden konnten.

Ein Krimineller hatte die E-Mail-Adresse des Betroffenen missbraucht, um einen ICQ-Account anzulegen, über den er kinderpornografische Schriften verbreitete. Auf Grund dessen wurden im Jahr 2014 gegen den Betroffenen zahlreiche Ermittlungsverfahren eingeleitet und betrieben. Erst nach einer Durchsuchung seiner Wohnung stellte die Polizei 2016 die Unschuld des Betroffenen fest.

Die Einleitung der Verfahren und die weitere Verarbeitung der personenbezogenen Daten war für den Betroffenen besonders einschneidend, da seine berufliche Tätigkeit eine jährliche Sicherheitsüberprüfung mit sich brachte. Entsprechende Stellenangebote konnte er nicht annehmen, denn der zu erwartende Reputationsschaden wäre bei einem negativen Bescheid aus der Sicherheitsüberprüfung enorm gewesen.

Berufsfreiheit stark eingeschränkt

Zudem wurde die Löschung der personenbezogenen Daten aus dem Vorgangssystem der Polizei auf ein Datum im Jahr 2027 festgelegt. Durch die Ermittlungen und die lange Speicherdauer war die Berufsfreiheit des Betroffenen erheblich eingeschränkt.

Datenschutzbeauftragte erst spät eingeschaltet

Der Betroffene erhob deshalb Klage vor dem zuständigen Verwaltungsgericht. Am 2. April 2019 wurde ich gemäß § 65 der Verwaltungsgerichtsordnung beigeladen und erhielt so Kenntnis über den Sachverhalt. Zu diesem Zeitpunkt lag die erste Verarbeitung der personenbezogenen Daten des Betroffenen bereits fünf Jahre zurück.

In meiner Stellungnahem teilte ich im Mai 2019 dem Verwaltungsgericht mit, dass für die weitere Speicherung der personenbezogenen Daten des Betroffenen bis zum Jahre 2027 keine Rechtsgrundlage vorliegen würde. Durch die zweifelsfrei erwiesene Unschuld des Betroffenen wäre die Speicherung in diesem Fall nicht mehr erforderlich. Der Klage auf Löschung der personenbezogenen Daten sei deshalb stattzugeben. Nach weiterer Beratung durch meine Behörde löschte die verantwortliche Polizeidirektion die Daten des Klägers. Daraufhin wurde der Rechtsstreit im Oktober 2019 durch den Kläger für erledigt erklärt.

J.2. Justiz

2.1 Abgrenzung justizieller Tätigkeit von Verwaltungsaufgaben

Im Justizbereich tritt immer wieder die Frage auf, ob einzelne Verarbeitungsvorgänge, gegen die sich Beschwerdeführer wenden, als justizielle Tätigkeit einzustufen sind. Ist das der Fall, hat dies zur Folge, dass die Landesbeauftragte für den Datenschutz (LfD) als Aufsichtsbehörde nicht zuständig ist.

Gesetzliche Grundlagen

Die Art. 55 Abs. 3 der Datenschutz-Grundverordnung (DS-GVO) und Art. 45 Abs. 2 der JI-Richtlinie enthalten Bestimmungen, wonach die Aufsichtsbehörden nicht für die Aufsicht über Verarbeitungen zuständig sind, die Gerichte im Rahmen ihrer justiziellen Tätigkeit vornehmen.

Zusätzlich findet sich in § 1 Abs. 2 des Niedersächsischen Datenschutzgesetzes (NDSG) die Regelung, dass für die Gerichte sowie für die Behörden der Staatsanwaltschaft die Vorschriften dieses Teils nur gelten, soweit sie Verwaltungsaufgaben wahrnehmen. In Verbindung mit § 19 Abs. 1 NDSG, wonach die LfD ihre Aufgaben als Aufsichtsbehörde nach der DS-GVO auch in Bezug auf die Vorschriften des ersten Teils des NDSG und andere datenschutzrechtlichen Bestimmungen wahrnimmt, ergibt sich ebenfalls diese einschränkende Zuständigkeit. Als Gegenstück zur justiziellen Tätigkeit wird dabei der Begriff der Verwaltungsaufgaben verwendet.

Reichweite justizieller Tätigkeit

Zum Begriff der justiziellen Tätigkeit stellt sich die Frage, ob dieser restriktiv aufzufassen ist, so dass nur die richterliche Tätigkeit als solche darunterfällt. Dann wäre die justizielle Tätigkeit angelehnt an die verfassungsrechtlich gewährleistete richterliche Unabhängigkeit zu sehen. Verwaltungsaufgaben wären demgegenüber sämtliche übrigen Datenverarbeitungen an den Gerichten, denen keine richterliche Würdigung zugrunde liegt; also solche, die nicht der richterlichen Unabhängigkeit unterfallen.

Anlehnung an richterliche Unabhängigkeit

Alternativ könnte der Begriff umfassender verstanden werden, so dass sämtliche Tätigkeiten, die mit gerichtlichen Verfahren in Verbindung stehen, dar-

unterfielen. Dann wären auch Tätigkeiten, die mit der Vorbereitung und der ausführenden Nachbearbeitung richterlicher Verfügungen verbunden sind (etwa die Tätigkeiten der Geschäftsstelle, ausgeführt durch Urkundsbeamte), umfasst. Ebenso kämen hier weitere, originär dem Aufgabenbereich des Richters zugeordnete Tätigkeiten in Betracht, die jedoch durch Gesetz anderen Personen, insbesondere Rechtspflegern, zur eigenständigen Wahrnehmung übertragen sind. Dies hätte eine weitgehende Einschränkung der Aufsichtsbefugnisse meiner Behörde zur Folge.

Enge Auslegung bevorzugt

Nach derzeitiger Einschätzung in meiner Behörde ist der Begriff der justiziellen Tätigkeit nicht derart umfassend zu verstehen. Stattdessen beschränkt sich der Begriff grundsätzlich auf die richterliche Tätigkeit als solche, die der richterlichen Unabhängigkeit unterliegt. Nur für den Bereich der richterlichen Entscheidungsfindung als Kernbereich der Judikative ist ein Ausschluss der Kontrolle durch meine Behörde gerechtfertigt. Eine darüberhinausgehende Beschränkung der Kontrollbefugnisse widerspricht den Grundsätzen der datenschutzrechtlichen Aufsicht. Demnach ist die Zuständigkeit der LfD als Aufsichtsbehörde gegenüber den öffentlichen Stellen üblicherweise gegeben. Es ist kein Grund ersichtlich, warum meine Behörde nicht auch für die Aufsicht über Verarbeitungen von personenbezogenen Daten zuständig sein soll, welche die Gerichte im Rahmen des „normalen Verwaltungsbetriebs" wie andere Behörden durchführen. In diesen Fällen ist eine Privilegierung der Gerichte nicht erforderlich.

Im Übrigen ist selbst der außerhalb meiner Zuständigkeit liegende Kernbereich der richterlichen Tätigkeit nicht völlig kontrolllos. Nach Erwägungsgrund (EG) 20 DS-GVO sollen unabhängige Stellen der Justiz diesbezüglich tätig werden. Diese Stelle müssen allerdings noch eingerichtet werden.

Einzelfall muss betrachtet werden

Nach meiner Auslegung wären also die übrigen Datenverarbeitungen als Verwaltungstätigkeiten einzustufen, wobei jeweils der Einzelfall zu berücksichtigen ist. Es wäre zum Beispiel denkbar, dass die Geschäftsstelle den Inhalt einer richterlichen Verfügung ausführt.

Gleiche Zielrichtung im Europarecht

Diese engere Auslegung des Begriffs dürfte auch dem Sinn und Zweck entsprechen, der mit den europarechtlichen Regelungen verfolgt wird. So nimmt der EG 80 der JI-Richtlinie explizit auf die richterliche Unabhängigkeit Bezug. Dieser formuliert in den Sätzen 1 und 2:

„Obgleich diese Richtlinie auch für Tätigkeiten der nationalen Gerichte und anderer Justizbehörden gilt, sollte sich die Zuständigkeit der Aufsichtsbehörde nicht auf die von Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Datenverarbeitungen erstrecken, damit die Unabhängigkeit der Richter bei der Ausübung ihrer richterlichen Aufgaben gewahrt bleibt.

Diese Ausnahme sollte allerdings begrenzt werden auf justizielle Tätigkeiten in Gerichtssachen und sich nicht auf andere Tätigkeiten beziehen, mit denen Richter nach dem Recht der Mitgliedstaaten betraut werden können."

Eine zu Satz 1 ähnlich lautende Erwägung findet sich in EG 20 der DS-GVO.

Auch auf europäischer Ebene deutet sich an, dass der überwiegende Teil der Datenschutzaufsichtsbehörden zur gleichen Auffassung wie mein Haus gelangt ist. Demnach sei der Begriff der justiziellen Tätigkeit nicht als umfassende Ausnahme zu verstehen. Eine konkrete Positionierung hierzu wird es voraussichtlich im Jahr 2020 geben.

J.3. Kommunalverwaltung

3.1 Prüfung zur Umsetzung der DS-GVO in Kommunen

Im November 2018 begann meine Behörde mit der Prüfung von 150 Kommunen in Niedersachsen zur Umsetzung der Datenschutz-Grundverordnung (DS-GVO), abgeschlossen wurde die Befragung im Juli 2019. Obwohl die Verordnung zu Beginn der Prüfung bereits ein halbes Jahr Geltung hatte, hatten vielen Kommunen noch nicht alle nötigen Anpassungsarbeiten beendet.

Vollständiger Prüfbericht: https://t1p.de/bericht-kommunen

Zur Durchführung dieser Prüfung hatte ich einen Fragebogen an 12 Landkreise, 3 kreisfreie Städte, 3 große selbstständige Städte, 42 Samtgemeinden und 90 Gemeinden geschickt. Ich wollte in Erfahrung bringen, vor welchen Problemen die Kommunen bei der Umsetzung der DS-GVO stehen. Die Prüfung bezog sich auf folgende Themenfelder:

1. Organisation,
2. datenschutzkonforme Verarbeitung,
3. Umgang mit Betroffenenrechten und
4. Umgang mit Datenschutzverletzungen.

Übergangsphase nicht ausreichend genutzt

Viele Kommunen hatten die zweijährige Übergangsphase zwischen Inkrafttreten und Geltung der DS-GVO nicht ausreichend genutzt. Als Folge hatten die befragten Stellen weder am 25. Mai 2018 (dem Geltungsbeginn) noch zum Zeitpunkt der Abfrage im November 2018 die erforderlichen Anpassungsarbeiten zur Umsetzung der DS-GVO abgeschlossen. Für den Abschluss der Arbeiten planten zahlreiche Kommunen noch auffallend viel Zeit ein.

Ergebnisse zeigen Licht und Schatten

Positiv: DSB und Auftragsverarbeitung

Als positiv stellte sich heraus, dass alle Kommunen ihrer Pflicht zur Benennung einer bzw. eines Datenschutzbeauftragten (DSB) nachgekommen waren. Es sind jedoch Zweifel angebracht, ob den Benannten in allen Fällen der zur Aufgabenerfüllung erforderliche Zeitanteil zur Verfügung steht. Ebenfalls erfreulich war, dass fast alle angeschriebenen Städte, Landkreise und Gemeinden inzwischen mit der Überprüfung ihrer Verträge zur Auftragsverarbeitung begonnen hatten.

Negativ war hingegen, dass erst acht Kommunen ein vollständiges Verzeichnis der Verarbeitungstätigkeiten (VVT) erstellt hatten. Dies ist besonders problematisch, da das VVT zentrales Steuerungselement einer gesetzmäßigen Datenverarbeitung ist. Auffällig war hier auch, dass die in den verschiedenen Verzeichnissen aufgeführte Zahl der Verarbeitungstätigkeiten sehr schwankte, auch wenn die Kommunen zum Teil nahezu identische Verwaltungsaufgaben wahrzunehmen hatten.

Informationspflichten nur zum Teil erfüllt

Bei der Sicherstellung der Betroffenenrechte ergab sich ein uneinheitliches Bild. Die Informationspflichten für das Internetangebot der Kommunen wurden nahezu vollständig durch entsprechende Datenschutzerklärungen auf den Webseiten erfüllt. Bei Datenerhebungen zum Zweck der übrigen Verwaltungstätigkeit hatten hingegen nur wenige Kommunen die notwendigen Anpassungsarbeiten zur Erfüllung der Informationspflichten abgeschlossen.

Datenschutz-Folgenabschätzung (DSFA) für Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bergen, lagen ebenfalls nur bei sehr wenigen Kommunen vor. 134 Kommunen hatten laut Befragung noch gar keine DSFA erstellt. Hier besteht also noch großer Handlungsbedarf.

Unter Geltung der DS-GVO müssen nun auch öffentliche Stellen Datenschutzverletzungen melden. Die notwendigen organisatorischen Maßnahmen zur Umsetzung dieser neuen Pflicht hatten aber nur 40 Kommunen ergriffen. Der überwiegende Teil der Befragten gab an, entsprechende Vorkehrungen im Laufe des Jahres 2019 abzuschließen.

Anforderungen bei den meisten nicht erfüllt

Als Gesamtergebnis bleibt festzustellen, dass die meisten der 150 angefragten Kommunen zum Zeitpunkt dieser Prüfung noch nicht die Anforderungen der DS-GVO erfüllt hatten. Der größte Nachholbedarf offenbarte sich bei den Fragen zur Durchführung von Datenschutz-Folgenabschätzungen sowie bei der Bearbeitung von Datenpannen.

Große Kommunen, wie z. B. Landkreise, waren im Übrigen nicht unbedingt besser aufgestellt als kleinere Verwaltungseinheiten. Dies legt die Schlussfolgerung nahe, dass es bei der Umsetzung der Datenschutz-Grundverordnung und der mit ihr einhergehenden Änderungen auch darauf ankommt, wie intensiv sich die Behördenleitung mit der Rechtsmaterie auseinandersetzt.

Wie geht es weiter?

Weitere Prüfungen geplant

Ich werde im Kommunalbereich weitere Prüfungen durchführen. Ziel ist es, dass alle Landkreise, kreisfreien Städte, großen selbstständigen Städte, Samtgemeinden und Gemeinden in den kommenden Jahren geprüft werden. Die Themen werden je nach Aktualität angepasst und durch bereichsspezifische Komplexe ergänzt. Auch bereits geprüfte Kommunen müssen damit rechnen, in eine erneute Prüfung einbezogen zu werden.
Des Weiteren werde ich anlassbezogen von den Kommunen Auszüge aus deren VVT sowie DSFA anfordern, sofern bei mir eingehende Beschwerden dies notwendig machen.

3.2 Live-Streaming von Ratssitzungen

Live-Streams von Ratssitzungen dienen dazu, demokratische Abstimmungsprozesse auf kommunaler Ebene transparenter zu machen. Zudem sollen die in den Sitzungen diskutierten Inhalte einer größeren Zahl von Bürgerinnen und Bürgern nähergebracht werden. Für ein rechtmäßiges Streaming sind allerdings die Bestimmungen des Datenschutzes einzuhalten. Die Landeshauptstadt Hannover bat mich im August 2019 darum, dazu im Organisations- und Personalausschuss Stellung zu nehmen.

Grundrechte der Betroffenen vor Ort beachten

Live-Streams von Ratssitzungen können – gerade in Zeiten aufkeimender Politikverdrossenheit – die demokratische Basis stärken und das allgemeine Interesse der Bürgerinnen und Bürger an Politik fördern. Gleichwohl müssen bei allen Vorteilen, die das Streaming mit sich bringt, auch die Grundrechte derer beachtet werden, die in der Ratssitzung entweder als Mandatsträger Rede und Antwort stehen oder als Interessierte aus dem Publikum heraus die Sitzung verfolgen.

Im Zuge des Live-Streamings werden personenbezogene Daten verarbeitet. Die Rechtmäßigkeit dieser Verarbeitung setzt eine gesetzliche Rechtsgrundlage oder die Einwilligung der jeweils betroffenen Person voraus. In Niedersachsen findet sich die Rechtsgrundlage für die Durchführung von Live-Streamings aus Ratssitzungen in § 64 Abs. 2 Satz 2 Niedersächsisches Kommunalverfassungsgesetz (NKomVG). Demnach sind Bild- und Tonaufnahmen von Mitgliedern der Vertretung mit dem Ziel der Berichterstattung zulässig, wenn die Hauptsatzung der Kommune eine entsprechende Regelung enthält.

Transparenz, aber nicht um jeden Preis

Aus datenschutzrechtlicher Sicht muss insbesondere beachtet werden, dass keine Aufnahmen von Personen gemacht werden, die nicht Mitglieder der Vertretung sind, also zum Beispiel von Zuschauerinnen und Zuschauern. Von diesen muss immer vor Beginn der Bild- und/oder Tonaufnahmen eine Einwilligung eingeholt werden. Doch auch die Mandatsträgerinnen und Mandatsträger können verlangen, dass ihre Redebeiträge nicht übertragen werden (§ 64 Abs. 2 Satz 3 NKomVG). Kommunen sollten organisatorische Vorkehrungen treffen, welche die praktische Umsetzung dieses Rechts ermöglichen. Dies könnte etwa ein optisches oder akustisches Signal an den Aufnahmeleiter sein, das per Knopfdruck durch die Mandatsträger ausgelöst wird oder auch das Heben einer farbigen Karte.

Mandatsträger können sich gegen Aufnahme entscheiden

Echte Live-Übertragung oder Mediathek?

Abschließend möchte ich darauf hinweisen, dass sich die Kommunen bei ihrer Entscheidung zum Einsatz von Live-Streaming entscheiden müssen, ob die Übertragung mit dem Ende der Sitzung tatsächlich gestoppt wird und es somit bei einer wortwörtlichen Live-Übertragung bleibt oder ob eine Aufzeichnung weiterhin in einer Mediathek zum Abruf bereitgestellt werden soll. Steht die Aufzeichnung weiterhin zum Abruf bereit, sollte ein Löschkonzept sicherstellen, dass diese nur so lange abgerufen werden kann, wie es auch erforderlich ist. Über die Erforderlichkeit entscheidet die jeweilige Kommune eigenverantwortlich.

Denkbar wäre, dass die Aufzeichnung einer vorangegangenen Sitzung gelöscht wird, sobald die Aufzeichnung der nächsten Sitzung zum Abruf bereitgestellt wird. Eine darüber hinaus gehende Speicherdauer, etwa zur Nachverfolgung politischer Prozesse, die sich über mehrere Sitzungen hinziehen, sollte in der Hauptsatzung entsprechend begründet werden.

Bei allen Vorteilen gilt es grundsätzlich zu bedenken, dass Daten, die über das Internet veröffentlicht werden, nicht ohne Weiteres vollständig gelöscht werden können. Denn es kann nie ganz ausgeschlossen werden, dass die Daten kopiert und weiterverbreitet werden.

3.3 Ratsinformationssysteme rechtmäßig einsetzen

Viele Kommunen nutzen mittlerweile Ratsinformationssysteme (RiS). Diese können die Arbeit des Rates erleichtern und demokratische Prozesse auf kommunaler Ebene transparenter gestalten. Sie bieten aber auch die Möglichkeit, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten. Im Berichtszeitraum haben meine Behörde zahlreiche Beschwerden erreicht, die sich auf die Veröffentlichung von Daten in dem für die Öffentlichkeit bestimmten Teil des RiS beziehen.

Ratsinformationssysteme bündeln die für die Ratsarbeit relevanten Informationen und dienen einer effizienteren Vor- und Nachbereitung der Sitzungen. Sie erleichtern so die Arbeit der Ratsmitglieder. Daneben tragen RiS zur politischen Willensbildung bei, indem sie demokratische Prozesse transparent machen und so die Bürgerinnen und Bürger am politischen Geschehen teilhaben lassen. So können sich sowohl die Mandatsträger als auch die Bürger über die zur Beratung oder Beschlussfassung anstehenden Themen umfassend informieren.

Vertraulichkeit und Integrität wahren

Mithilfe von RiS lassen sich aber auch personenbezogene Daten zielgerichtet auswerten und verarbeiten. Eine Akzeptanz der Systeme als Bestandteil einer offenen und bürgernahen Informationskultur kann daher nur geschaffen werden, wenn die Grundsätze von Vertraulichkeit und Integrität bei deren Einsatz gewahrt werden.

Transparenz durch öffentlichen Bereich

Klassischerweise besteht ein RiS aus einem nicht-öffentlichen Teil, der ausschließlich den Vertretern der kommunalen Gremien zugänglich ist, und einem über das Internet für alle Bürgerinnen und Bürger öffentlich einsehbaren Bereich.

Der nicht-öffentliche Bereich dient vor allem der Vor- und Nachbereitung der Ratssitzungen. Hierzu gehören unter anderem die Sitzungsplanung, die Erstellung von Tagesordnung und Einladungen, die Ausfertigung von Beschlüssen, die Erstellung und Archivierung von Vorlagen sowie der Niederschriften vergangener Sitzungen, bis hin zur Verwaltung von Sitzungsgeldern. Der öffentliche Bereich dient der Information der Bürgerinnen und Bürger. Durch die Veröffentlichung von Einladungen zu den Ratssitzungen, der dazugehörigen Beschlussvorlagen und der Niederschriften wird die kommunale Politik transparent und bürgernah gestaltet.

Datenschutzrechtliche Rahmenbedingungen

Verarbeitung fällt unter Regelungen der DS-GVO

Die vielfältigen Einsatzmöglichkeiten von RiS lassen erahnen, dass erhebliche Datenmengen in einem solchen System verwaltet werden können. Viele Dokumente enthalten personenbezogene Daten, sodass auch datenschutzrechtliche Aspekte beim Einsatz von RiS berücksichtigt werden müssen. Unabhängig davon, ob personenbezogene Daten im internen oder externen Bereich veröffentlicht werden, liegt eine Verarbeitung im Sinne von Art. 4 Nr. 2 Datenschutz-Grundverordnung (DS-GVO) vor.

Für die Verarbeitung personenbezogener Daten müssen insbesondere die folgenden Grundsätze beachtet werden:

Rechtmäßigkeit der Verarbeitung
Die Daten dürfen nur verarbeitet werden, wenn es eine gesetzliche Grundlage gibt oder die Einwilligung der betroffenen Person vorliegt (Art. 5 Abs. 1 Buchstabe a) DS-GVO).

Datenminimierung
Die Verarbeitung ist auf das erforderliche Maß zu beschränken (Art. 5 Abs. 1 Buchstabe c) DS-GVO).

Speicherbegrenzung
Es ist ein Löschkonzept zu entwickeln, in dem festgelegt ist, für welche Dauer die im RiS vorhandenen Dokumente, die personenbezogene Daten enthalten (z. B. Protokolle von Ratssitzungen), gespeichert, wann sie gelöscht werden (Art. 5 Abs. 1 Buchstabe e) DS-GVO) und für welchen Zeitraum sie öffentlich zugänglich sind.

Technisch-organisatorische Schutzmaßnahmen
Die personenbezogenen Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet (Artikel 5 Abs. 1 Buchstabe f) DS-GVO). Dazu zählt auch, dass die Daten vor unbefugter oder unrechtmäßiger Verarbeitung geschützt werden. Vor der Einführung eines RiS ist ggf. eine Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) nötig.

Datenschutzrechtliche Stolperfallen

Vorsicht bei Publikationen im öffentlichen Bereich des RiS

Grundsätzlich sind die Sitzungen des Rates öffentlich. Dieser Öffentlichkeitsgrundsatz, der auf dem in Art. 28 Abs. 1 Grundgesetz verankerte Demokratieprinzip fußt, gilt jedoch nicht grenzenlos. Er wird durch das Recht auf informationelle Selbstbestimmung eingeschränkt. Wenn also berechtigte private Interessen einzelner Personen überwiegen, ist die Öffentlichkeit von der Sitzung auszuschließen.

Ein häufig vorkommender datenschutzrechtlicher Verstoß ist die versehentliche Veröffentlichung personenbezogener Daten in Dokumenten im öffentlich zugänglichen Bereich des RiS. Dies kann etwa bei der Nennung von Namen und Adressen von Personen der Fall sein, die Einwendungen im Rahmen von Bauleitverfahren eingereicht haben. In diesen Fällen mangelt es an der Rechtmäßigkeit der Verarbeitung.

Auch Niederschriften über den öffentlichen Teil der Sitzung enthalten häufig personenbezogene Daten oder zumindest lässt sich mithilfe weiterer Quellen ein Personenbezug herstellen. Vor jeder

Veröffentlichung von Dokumenten im öffentlichen Teil des RiS sollte die verantwortliche Kommune daher genau prüfen, ob die Unterlagen personenbezogene Daten enthalten und ob die entsprechenden Passagen anonymisiert werden müssen. Nur so lässt sich ein Verstoß gegen den Grundsatz der Rechtmäßigkeit der Verarbeitung vermeiden.

Kein pauschaler Zugriff

Der interne Bereich des RiS wird von vielen Personen aus unterschiedlichen Bereichen der Verwaltung zu verschiedensten Zwecken genutzt. Umso wichtiger ist es, dass der Zugriff nicht pauschal gewährt wird, sondern klar geregelt ist. Dafür ist ein Berechtigungskonzept nötig, in dem festgelegt ist, welche Personen auf welche Bereiche zugreifen dürfen.

Rechte-Rollen-Konzept entwickeln

Die Vergabe von Zugriffsrechten soll sicherstellen, dass nur berechtigte Personen im Rahmen der ihnen zustehenden Befugnisse die für ihre Tätigkeit erforderlichen Daten einsehen und bearbeiten können. Ein sogenanntes „Rechte-Rollen-Konzept" stellt eine technisch-organisatorische Maßnahme dar, um dem Grundsatz der Erforderlichkeit Genüge zu tun.

Auftragsverarbeitung nur mit Vertrag

Werden externe Dienstleister mit der Einrichtung eines RiS und der Haltung der dort gespeicherten Daten auf eigenen Servern beauftragt, so liegt eine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO vor. Die verantwortliche Kommune ist dann verpflichtet, einen Vertrag mit dem Dienstleister zu schließen, der die Voraussetzungen des Art. 28 DS-GVO erfüllt. Für die Verarbeitung der personenbezogenen Daten bleibt die Kommune weiterhin verantwortlich.

Fazit: Der Einsatz von RiS trägt entscheidend dazu bei, demokratische Abstimmungsprozesse auf kommunaler Ebene transparenter zu gestalten und die in den Ratssitzungen diskutierten Inhalte einer größeren Anzahl von Bürgerinnen und Bürgern näher zu bringen. Gleichwohl darf bei allen Vorteilen das Recht auf informationelle Selbstbestimmung nicht außer Acht gelassen werden.

3.4 Bau(recht)stelle im Internet

Im Jahr 2019 beschwerten sich vermehrt Bürgerinnen und Bürger über Datenschutzverstöße bei Bebauungsplanverfahren. Bei festgestellten Verstößen habe ich Verwarnungen ausgesprochen.

Bereits zum Jahreswechsel gingen bei mir die ersten Beschwerden zum Baurecht ein. Die Betroffenen erklärten, dass eine Kommune ihre Vornamen, Namen, Straße, Hausnummer, Wohnort und Unterschriften im Internet veröffentlicht habe. Weitere Hinweise auf ähnliche Datenschutzverstöße habe ich über das Jahr verteilt erhalten. In den meisten Fällen wurden Daten über die Webseiten oder den öffentlichen Teil der Ratsinformationssysteme (RiS) der Kommunen veröffentlicht.

Beteiligung der Öffentlichkeit - Schwärzungen versäumt

Hintergrund war in allen Fällen, dass nach dem Baugesetzbuch (BauGB) die Öffentlichkeit möglichst frühzeitig an der Planung von Bauvorhaben zu beteiligen ist (§ 3 BauGB). Im Rahmen dieser Beteiligung besteht die Möglichkeit, Stellungnahmen abzugeben (§ 3 Abs. 2 BauGB). Hiervon hatten die Betroffenen Gebrauch gemacht.

Für die Beschlussfassung werden den Ratsmitgliedern die Inhalte der eingegangenen Stellungnahmen zur Verfügung gestellt und mit Hinweisen der Kommune versehen. Hierfür wird meist das RiS genutzt. Dort werden die Einladungen zu den Sitzungen mit den dazugehörigen Anlagen bereitgestellt. In den meisten mir vorliegenden Fällen wurde versäumt, die erforderlichen Schwärzungen vorzunehmen. Fast alle Kommunen haben die fehlerhaften Dokumente entweder selbstständig, nach Meldung einer Datenschutzverletzung oder auf meinen Hinweis hin sofort entfernt und durch neue, datenschutzkonforme ersetzt.

Fast alle Kommunen korrigieren Fehler

Prüfung von Stichproben

Aufgrund der stark angestiegenen Beschwerdezahl in diesem Bereich habe ich stichprobenartig die auf den Webseiten bzw. im öffentlichen Teil der RiS vorhandenen Dokumente zu Bauleitverfahren überprüft. In fast allen geprüften Dokumenten wurden die datenschutzrechtlichen Anforderungen berücksichtigt. Bei Auffälligkeiten nahm meine Behörde mit der betroffenen Kommune Kontakt auf. Dies hatte fast immer zur Folge, dass die Dokumente angepasst wurden.

Namensnennung im öffentlichen Interesse?

Kommune: Veröffentlichung für Entscheidung des Rates nötig

Eine Kommune teilte mir allerdings mit, dass sie nicht beabsichtige, Schwärzungen vorzunehmen. Begründet wurde dies damit, dass es sich bei der öffentlichen Beteiligung im Bauleitverfahren um einen demokratischen Meinungsbildungsprozess handele, bei dem der Datenschutz des Einzelnen nicht der ausreichenden Information und Handlungsfähigkeit der Vertretung sowie der Öffentlichkeit übergeordnet ist. Dies ergäbe sich bereits aus der angeordneten Beteiligung der Öffentlichkeit. Von Personen, die sich an der Aufstellung von Ortsrecht beteiligen, könnten auch Vor- und Nachnamen sowie die Anschrift veröffentlicht werden, da dies für die Entscheidungsfindung des Rates von Bedeutung sein kann.

Diesen Ausführungen konnte ich nicht ohne Weiteres folgen, zumal außer dieser allgemeinen Betrachtung keine Rechtsgrundlagen genannt wurden, die die Verarbeitung hätten rechtfertigen können. Es ergaben sich somit Zweifel, ob die Grundsätze der Verarbeitung (Art. 5 Abs. 1 DS-GVO), insbesondere die Rechtmäßigkeit der Verarbeitung, eingehalten wurden. Die Rechtmäßigkeitsvoraussetzungen für die Verarbeitung werden in Art. 6 DS-GVO benannt. Kommunen haben zu berücksichtigen, dass es grundsätzlich einer Rechtsgrundlage für die Verarbeitung personenbezogener Daten bedarf (Art. 6 Abs. 1 i.V.m. Art. 6 Abs. 2 DS-GVO). Das sogenannte Verbot mit Erlaubnisvorbehalt besteht unter der DS-GVO fort.

Kommune folgt Argumentation der LfD

Verarbeitung war nicht rechtmäßig

Ich nahm diesen Fall zum Anlass, von der Kommune eine Stellungnahme nach § 20 Abs. 2 Niedersächsisches Datenschutzgesetz (NDSG) anzufordern. Bei diesem förmlichen Verfahren wird auch die zuständige Rechts- oder Fachaufsichtsbehörde (also entweder das Niedersächsische Innenministerium oder der jeweilige Landkreis) der Kommune beteiligt. In der Aufforderung zur Stellungnahme wies ich darauf hin, dass eine Veröffentlichung personenbezogener Daten von Personen, die eine Stellungnahme im Bauleitverfahren abgeben, weder vom BauGB noch vom NDSG erlaubt wird. Auch enthält das Niedersächsische Kommunalverfassungsgesetz keine entsprechende Erlaubnis. Das BauGB sieht zwar eine Internetveröffentlichung des Bebauungsplanes mit der Begründung und der zusammenfassenden Erklärung vor (§ 10 Abs. 2 BauGB), jedoch umfasst diese nur die Erläuterung der Sachargumente im Rahmen des Abwägungsprozesses (§ 10 Abs. 1 BauGB). Damit war bereits die Rechtmäßigkeit der Verarbeitung nicht gegeben und keine weitergehende Prüfung nötig.

Zwischenzeitlich hat mir die betroffene Kommune mitgeteilt, dass sie meiner Argumentation folgt und die Vorlagen an die datenschutzrechtlichen Erfordernisse anpasst.

3.5 Datenschutz im Vorfeld von Wahlen

Im Vorfeld von Wahlen müssen datenschutzrechtliche Vorkehrungen getroffen werden. Dass dies nicht immer in ausreichendem Maß geschieht, zeigen die Eingaben, die ich in Bezug auf die Europa- und eine Bürgermeisterwahl erhielt.

Europawahl – falscher Umschlag für Wahlschein

Muster verwendet, aber Fenster zu groß

Im Zusammenhang mit der Europawahl 2019 erreichte mich folgende Beschwerde: Eine Gemeinde hatte den Wahlschein im verschlossenen Briefumschlag so versandt, dass durch das Adressfenster des Umschlags das Geburtsdatum des Wahlberechtigten sichtbar war. Im Rahmen meines Kontrollverfahrens teilte mir die Gemeinde mit, dass die Gestaltung des Wahlscheins dem gesetzlich vorgeschriebenen Muster entsprochen habe. Allerdings sei ein zu großer Umschlag verwendet worden, so dass der Wahlschein verrutschen konnte.

Die Gemeinde änderte die Umschlagsgröße aufgrund meines Kontrollverfahrens zeitnah. Da es sich zudem bei dem Geburtsdatum nicht um Daten aus dem sensitiven Bereich im Sinne von Art 9 der Datenschutz-Grundverordnung (DS-GVO) handelt, habe ich von einer Maßnahme gegenüber der Kommune abgesehen.

Bürgermeisterwahl – auch Unterlagen im Vorfeld sind sensibel

Nur Ausschuss darf Unterstützungsliste sehen

Eine weitere Beschwerde erhielt ich im Zusammenhang mit einer Bürgermeisterwahl. In einer Gemeinde trat im Vorfeld der Wahl der Gemeindewahlausschuss zusammen. Die Sitzung war nötig, um die Liste der Bürgermeisterkandidaten entsprechend der gesetzlichen Vorschriften aufzustellen. Die Unterlagen der potenziellen Kandidaten waren Gegenstand der Sitzung. Es handelte sich um eine öffentliche Sitzung; die Zuschauer saßen in ausreichendem Abstand zum Ausschuss.

Am Tisch des Gemeindewahlausschusses hatten auch die vom Niedersächsischen Kommunalwahlgesetz vorgesehenen Vertrauenspersonen der Bürgermeisterkandidaten Platz genommen. Diese sind wie Vertreter befugt, Erklärungen abzugeben und entgegenzunehmen. Gegenstand der Wahlvorschläge, die auf der Sitzung geprüft wurden, war auch die Wahlunterstützungsliste für einen Einzelbewerber. Diese Liste ist nur zur Einsicht durch den Gemeindewahlausschuss vorgesehen. Allerdings hatten auch die Vertrauenspersonen, die nicht dem Ausschuss angehören, die Möglichkeit darauf zuzugreifen. Schon diese Zugriffsmöglichkeit stellt einen Datenschutzverstoß dar. Ich habe daher gegenüber der Gemeinde eine Verwarnung gemäß DS-GVO ausgesprochen.

J.4. Allgemeine Landesverwaltung

4.1 Prüfung der Landesaufnahmebehörde Niedersachsen

Im Rahmen der Unterbringung und Betreuung von Asylsuchenden arbeitet die Landesaufnahmebehörde Niedersachsen (LAB NI) mit externen Dienstleistern zusammen. Bereits in meinem Tätigkeitsbericht 2015/2016 habe ich die Beratung Dritter erläutert, wonach eine Auftragsverarbeitung vorliegt, wenn diese personenbezogene Daten für die LAB NI verarbeiten. Ich habe diesen Umstand zum Anlass genommen, den Abschluss entsprechender Verträge zu überprüfen.

Die von LAB NI eingesetzten Dienstleister verarbeiten im Rahmen ihrer Tätigkeit personenbezogene Daten der Asylsuchenden im Auftrag. Datenschutzrechtlich verantwortlich ist die Landesaufnahmebehörde. Voraussetzung für den Einsatz von sogenannten Auftragsverarbeitern ist jedoch der Abschluss eines entsprechenden Vertrags zwischen dem Verantwortlichen und dem eingesetzten Dienstleister (Art. 28 Datenschutz-Grundverordnung (DS-GVO)).

Nötige Verträge fehlen

Mein Prüfverfahren hat ergeben, dass die LAB NI an verschiedenen Standorten externe Dienstleister als Auftragsverarbeiter einsetzt, ohne mit diesen entsprechende Verträge über die Auftragsverarbeitung abgeschlossen zu haben. Damit verstößt sie gegen die Vorgaben der DS-GVO. Ich habe deshalb gegenüber der LAB NI in 26 Fällen eine Verwarnung gemäß Art. 58 Abs. 2 lit. b) DS-GVO ausgesprochen. Im Zuge des Prüfverfahrens hat die Behörde ausdrücklich zugesagt, entsprechende Verträge unverzüglich abzuschließen. Ich werde die Angelegenheit weiterhin verfolgen, um die Einhaltung dieser Zusage zu überprüfen.

J.5. Schule

5.1 Prüfungen zu „WhatsApp“ und Klassenbüchern

Digitale Kommunikationsmittel werden in Schulen zunehmend wichtiger. Über den Beginn meiner Prüfung zum Einsatz von WhatsApp habe ich bereits in meinem Tätigkeitsbericht 2017/2018 informiert. Diese wurde nun abgeschlossen, genau wie eine Prüfung zu elektronischen Klassenbüchern.

Merkblatt: https://t1p.de/whatsapp-schule

Gegenstand der WhatsApp-Prüfung an 70 Schulen waren die Kommunikationswege, die zwischen den einzelnen Personengruppen (Lehrkräfte, Schülerinnen und Schüler, Eltern) genutzt werden. Ich wollte herausfinden, ob das von mir ausgesprochene Verbot der Nutzung des Messengers eingehalten wird. Ich hatte dies im „Merkblatt für die Nutzung von WhatsApp in Schulen“ erläutert.

Bequem und schnell, aber unzulässig

Die Prüfung hat ergeben, dass WhatsApp an zehn Schulen vor allem zur Kommunikation der Lehrkräfte untereinander, aber auch zwischen den Lehrkräften und den Schülerinnen und Schülern eingesetzt wurde. Dies mag für den Einzelnen bequem sein, ist aber aus datenschutzrechtlicher Sicht für die dienstliche Kommunikation unzulässig. Das ergibt sich unter anderem daraus, dass mit der Anmeldung bei WhatsApp automatisch alle im Mobiltelefon gespeicherten Kontakte an die WhatsApp Inc. übertragen werden. Dabei ist nicht sichergestellt, dass alle Kontakte ihre datenschutzrechtliche Einwilligung in die Weitergabe ihrer Daten erteilt haben.

Die übrigen 60 Schulen nutzten WhatsApp nicht. Das zeigt, dass das Merkblatt zur WhatsApp-Nutzung flächendeckend Beachtung findet und im Zuge dessen das Datenschutzniveau an den niedersächsischen Schulen gesteigert wurde. Ich habe die Schulen, die WhatsApp eingesetzt haben, im Rahmen der Prüfung auf das bestehende Verbot hingewiesen und mir die Untersagung des weiteren Einsatzes durch die Schulleitung schriftlich erklären lassen.

Einsatz von elektronischen Klassenbüchern

Auch zum Einsatz elektronischer Klassenbücher wurden 70 Schulen einer stichprobenhaften Überprüfung unterzogen. Gegenstand war einerseits, ob an den Schulen überhaupt elektronische Klassenbücher eingesetzt werden. War das der Fall ging es andererseits um die Frage, ob die Vorgaben der von mir veröffentlichten „Hinweise zur Einführung eines elektronischen Klassenbuchs" eingehalten werden.

Hinweise zu Klassenbüchern: https://t1p.de/elek-klassenbuch

Grundsätzlich ist die Einführung eines elektronischen Klassenbuchs gemäß § 31 Abs. 1 Niedersächsisches Schulgesetz (NSchG) rechtlich zulässig. Es ist jedoch darauf zu achten, dass nur die Daten erhoben werden, die auch für das Klassenbuch in Papierform erforderlich sind.

Wenn sich die Schule entscheidet, ein elektronisches Klassenbuch einzusetzen, muss dieses gemäß Art. 30 der Datenschutz-Grundverordnung (DS-GVO) in das Verzeichnis von Verarbeitungstätigkeiten aufgenommen werden. Vor der Einführung eines elektronischen Klassenbuchs ist zudem gemäß Art. 35 DS-GVO eine Datenschutz-Folgenabschätzung durchzuführen. Wenn die Datenverarbeitung nicht in der Schule stattfindet, sondern ein Dienstleister damit beauftragt wird, muss auch ein Auftragsverarbeitungsvertrag (Art. 28 DS-GVO) abgeschlossen werden.

Nur wenige Schulen nutzen das E-Klassenbuch

Von den 70 befragten Schulen nutzten nur 7 ein elektronisches Klassenbuch. Mit Ausnahme der Speicherung von Fotos der Schülerinnen und Schüler wurde der erforderliche Datenrahmen grundsätzlich eingehalten. In zwei Fällen lag zudem die erforderliche Datenschutz-Folgenabschätzung nicht oder nicht vollständig vor, an einer Schule fehlte ein notwendiger Auftragsverarbeitungsvertrag.

Ich habe die betroffenen Schulen auf die festgestellten Mängel hingewiesen und mir von ihnen schriftlich erklären lassen, dass diese abgestellt wurden.

5.2 Neue Regeln für private IT-Geräte von Lehrkräften

Bereits Ende 2017 ist der Erlass zur Verarbeitung personenbezogener Daten auf privaten IT-Geräten von Lehrkräften außer Kraft getreten. Im Berichtszeitraum hat das Niedersächsische Kultusministerium eine Neufassung auf den Weg gebracht. Dabei hat das Ministerium mehrere Änderungen formuliert, die ich zu großen Teilen aus datenschutzrechtlicher Sicht mitgetragen habe.

Einsatz privater Geräte stark reglementiert

Der Runderlass „Verarbeitung personenbezogener Daten auf privaten informationstechnischen Systemen (IT-Systemen) von Lehrkräften“ vom 01.02.2012 regelte, unter welchen Voraussetzungen Lehrerinnen und Lehrer ihre privaten IT-Geräte für dienstliche Zwecke nutzen durften. Der Einsatz privater Geräte ist grundsätzlich möglich, jedoch an strikte Voraussetzungen bei der Datenspeicherung geknüpft und nur in einem bestimmten Rahmen datenschutzrechtlich zulässig.

Bei den Änderungen in der Entwurfsfassung handelt es sich im Wesentlichen um die folgenden Punkte:

- Nutzung privater mobiler Endgeräte nur für die Eingabe und Anzeige personenbezogener Daten auf den gesicherten Servern der Schule oder einer beauftragten Stelle.

- Ergänzung des zulässigen Datenrahmens um die Fehlzeiten der Schülerinnen und Schüler sowie um personenbezogene Gesundheitsdaten i.S.v. Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO), die für die Erstellung eines Fördergutachtens zur Feststellung sonderpädagogischen Unterstützungsbedarfs erforderlich sind.

- Wegfall des Zutrittsrechts meiner Behörde in den häuslichen Bereich der Lehrkraft.

Ich begrüße, dass die Neufassung Klarheit schafft, indem sie zwischen Desktop-PCs und mobilen Endgeräten (Smartphones/Tablets) differenziert. Für die Verarbeitung personenbezogener Daten auf mobilen Endgeräten regelt der Erlass, dass diese nicht auf dem Festspeicher des Endgeräts selbst, sondern ausschließlich auf einem gesicherten Server der Schule oder dem Server einer hierfür beauftragten dritten Stelle vorgenommen werden darf. Damit wurde eine wesentliche Forderung meiner Behörde umgesetzt.

Keine Daten auf dem Speicher des privaten Geräts

Kontrollmöglichkeit in der Schule reicht aus

Ich habe auch mitgetragen, dass das Zutrittsrechts der Landesbeauftragten für den Datenschutz in den häuslichen Bereich der Lehrkraft wegfallen soll. Entscheidend für die Ausübung meiner Kontrollbefugnisse ist der Zugang zu den eingesetzten privaten IT-Systemen und Speichermedien. Das kann auch in den Diensträumen der jeweiligen Schule geschehen, sodass ein Zugang zu den Privaträumen der Lehrkräfte nicht erforderlich ist.

Schutz besonders sensibler Schülerdaten

Für nicht akzeptabel halte ich jedoch die Erweiterung des zulässigen Datenrahmens um Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO von Schülerinnen und Schülern zur Feststellung eines sonderpädagogischen Unterstützungsbedarfs. Die Verarbeitung besonderer Kategorien personenbezogener Daten stellt in Bezug auf die Sicherheit der Verarbeitung höhere Anforderungen an die zu treffenden technischen und organisatorische Maßnahmen. Diesen Anforderungen genügen private mobile Endgeräte grundsätzlich nicht.

Die Kontrolle, ob die eingesetzten technischen und organisatorischen Maßnahmen eingehalten werden und stets auf dem aktuellsten Stand sind, obliegt der verantwortlichen Schule. Diese regelmäßige Kontrolle wäre mit einem umfassenden Zugriff auf jedes einzelne private mobile Endgerät verbunden und würde eine private Nutzung des Geräts faktisch unmöglich machen. Die sichere Verarbeitung besonderer Kategorien personenbezogener Daten auf privaten mobilen Endgeräten ist daher derzeit praktisch nicht umsetzbar.

Sichere Verarbeitung besonderer Kategorien nicht möglich

Die von mir mitgetragenen Änderungen des Erlasses führen dazu, dass Lehrkräfte flexibler und unabhängiger arbeiten können. Der Erlass trat am 1. Januar 2020 in Kraft.

5.3 Digitalisierung im Schulbereich – Lernen unterwegs und Bildungscloud

In Niedersachsen werden im Schulbereich zwei Digitalisierungsprojekte durchgeführt, für die ich meine Beratung angeboten habe. Im Fall der Online-Plattform „Digitales Lernen unterwegs" (DigLu) wurde diese Beratung in Anspruch genommen. Dagegen lag zur Niedersächsischen Bildungscloud bis zum Ende des Berichtszeitraumes noch kein prüffähiges Datenschutzkonzept vor.

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

Das Projekt DigLu ist Bestandteil der Strategie der Kultusminister-konferenz (KMK) „Bildung in der digitalen Welt". Kern des Konzepts ist das Angebot einer Lernplattform und einer Schulorganisations-Software für Kinder beruflich Reisender, auf die online zugegriffen werden kann (siehe dazu auch meinen Tätigkeitsbericht 2017-2018). Da Niedersachsen eines von sechs Pilot-Ländern des Projekts ist, hat mein Haus zusammen mit weiteren Aufsichtsbehörden das von einer Arbeitsgruppe der KMK vorgelegte Datenschutzkonzept rechtlich bewertet. Dabei wurden folgende überarbeitungsbedürftigen Punkte identifiziert:

- Konkretisierung der betroffenen Datensätze,
- Differenzierung der Datenflüsse im Hinblick auf die jeweiligen Rechtsgrundlagen,
- Anpassung der Einwilligungserklärungsformulare und der Auftragsverarbeitungsverträge sowie
- Umsetzung der Betroffenenrechte.

Die KMK-Arbeitsgruppe wurde gebeten, diese rechtlichen Vorgaben umzusetzen, damit die Plattform bereits in der Pilotphase den datenschutzrechtlichen Vorgaben entspricht.

Bildungscloud noch ohne Datenschutzkonzept

Bereits im Jahr 2016 habe ich dem Kultusministerium meine datenschutzrechtliche Unterstützung bei der Entwicklung einer Niedersächsischen Bildungscloud angeboten.

Meiner Behörde lag bis zum Ende des Berichtszeitraumes noch kein prüffähiges Datenschutzkonzept vor, obwohl ich das Kultusministerium mehrfach darauf hingewiesen habe, dass die Schulcloud auch im Pilotbetrieb datenschutzrechtlichen Anforderungen entsprechen muss.

5.4 Zusammenarbeit mit der Landesschulbehörde

Meine Behörde tauscht sich regelmäßig mit der Landeschulbehörde zu aktuellen Themen im Schulbereich aus. Dadurch können datenschutzrechtliche Problemstellungen auf effektive Weise gelöst und an die Schulen kommuniziert werden.

Zur Unterstützung der Schulen in Fragen des Datenschutzes hat die Landesschulbehörde an allen Regionalabteilungen Dezernenten für den Datenschutz eingerichtet. Diese beraten die Schulen individuell und unterstützen die Datenschutzbeauftragten bei der Erfüllung ihrer Aufgaben. Zudem findet ein Austausch zwischen der Landesschulbehörde und meinem Haus zu datenschutzrechtlichen Fragestellungen statt, beispielsweise in Form regelmäßiger Arbeitstreffen.

FAQ Datenschutz der Landesschulbehörde: https://t1p.de/faq-lsb

Gemeinsam mit der Landesschulbehörde habe ich im Berichtszeitraum eine Übersicht wiederkehrender Fragen und Antworten erstellt, die den Datenschutz im Schullalltag betrifft. Auf diese Weise lassen sich bereits viele Unsicherheiten und Fragen im Vorhinein klären. Die mit uns abgestimmte Beratungstätigkeit der Landesschulbehörde wirkt sich positiv aus. Insbesondere ist dadurch die Anzahl der Beratungsanfragen an meine Behörde deutlich zurückgegangen.

So führt die sich stets fortentwickelnde gute Zusammenarbeit mit der Landesschulbehörde insgesamt zu einer Steigerung des Datenschutzniveaus an niedersächsischen Schulen.

J.6. Wirtschaft

6.1 Prüfung von 50 Unternehmen zeigt zum Teil große Defizite

Die Umsetzung der Datenschutz-Grundverordnung (DS-GVO) gelingt niedersächsischen Unternehmen bisher nur teilweise. Das ist das Ergebnis der branchenübergreifenden Prüfung von Unternehmen, die meine Behörde Ende 2019 abschließen konnte.

Abschlussbericht der Prüfung: https://t1p.de/q-pruefung

Große und mittelgroße Unternehmen mit Hauptsitz in Niedersachsen sollten in der sogenannten Querschnittsprüfung darlegen, ob und wie sie die Regelungen der DS-GVO in der betrieblichen Praxis mit Leben füllen. In einer branchenübergreifenden Prüfung wurden Ende Juni 2018 50 Unternehmen angeschrieben, die Fragen zu zehn Bereichen des Datenschutzes beantworten sollten.

Im Vordergrund der Querschnittsprüfung stand die Aufklärung und Sensibilisierung der Unternehmen. Das Hauptanliegen war es zu identifizieren, ob und wo es bei den verantwortlichen Stellen bei der Umsetzung der DS-GVO noch Nachholbedarf gibt. Zudem sollte mit der Prüfung das Bewusstsein für den Datenschutz im Allgemeinen und die Vorschriften der neuen Verordnung im Speziellen gestärkt werden.

Vorrangiges Ziel der Prüfung war es damit auch nicht, möglichst viele Fehler zu finden und Bußgelder zu verhängen. Eines war aber von vorneherein klar: Sollten während der Prüfung gravierende Verstöße gegen die DS-GVO festgestellt werden, waren auch weitergehende Maßnahmen bis hin zur Verhängung eines Bußgeldes möglich.

Fragebogen zu zehn Komplexen

Checkliste: https://t1p.de/checkliste-dsgvo

Der Fragebogen der Prüfung basierte auf der Checkliste für kleine und mittelständische Unternehmen, welche die LfD Niedersachsen im November 2017 veröffentlicht hatte.

Fragebogen: https://t1p.de/qpruefung-fragen

Mit den zehn Fragenkomplexen der Querschnittsprüfung wurden die für Verantwortliche wesentlichen Bereiche der DS-GVO angesprochen. Die Fragen betrafen die Themen Verzeichnis von Verarbeitungstätigkeiten (VVT) und Rechtsgrundlagen, die Betroffenenrechte, den technischen Datenschutz, die Datenschutz-Folgenabschätzung (DSFA), die Auftragsverarbeitung, die Bestellpflicht für Datenschutzbeauftragte, die Meldepflichten sowie die Rechenschaftspflicht. Zudem sollten die Unternehmen generell darstellen, wie sie sich

auf die DS-GVO vorbereitet hatten, welche Unternehmensbereiche involviert waren und welche Maßnahmen initiiert wurden.

Besonderer Wert wurde bei der Konzeption der Fragen auf die Darstellung der Prozesse in den betroffenen Unternehmen gelegt. Gerade diese geben in besonderer Weise Aufschluss darüber, wie gut ein Verantwortlicher in der Lage ist, die Anforderungen der DS-GVO zu erfüllen, da die Prozesse die grundsätzliche Vorgehensweise und Methodik wiederspiegeln. Die Fragen wurden zudem bewusst offen gestellt, um den Unternehmen die Möglichkeit zu eröffnen, ihre Antworten auf ihre konkrete Situation und Größe anzupassen. Gleichzeitig sollten durch die Fragen Hinweise darüber eingeholt werden, wie weit die einzelnen Anforderungen der DS-GVO bei den Unternehmen bereits erkannt und prozessual umgesetzt worden waren. Denn ohne die Verankerung der datenschutzrechtlichen Anforderungen in konkrete Unternehmensprozesse, kann eine dauerhafte Erfüllung der Anforderungen nicht gewährleistet werden.

Umfangreicher Kriterienkatalog

Um die Antworten einheitlich bewerten zu können, wurde zu den zehn Fragekomplexen ein detaillierter Katalog aus circa 200 Einzelkriterien erarbeitet. Damit war auch eine weitere Hilfestellung bezweckt. Anhand der Kriterien sollte verdeutlicht werden, was ein Verantwortlicher alles zu beachten hat, um datenschutzkonform aufgestellt zu sein. Daher wurde der Katalog am Ende der Querschnittsprüfung veröffentlicht und so allen (niedersächsischen) Unternehmen zugänglich gemacht.

Kriterienkatalog: https://t1p.de/qpruefung-kriterien

Die Kriterien basieren auf den rechtlichen Anforderungen der DS-GVO. Im Hinblick auf das Ziel der Querschnittsprüfung, einen Überblick über den Umsetzungstand der DS-GVO zu erhalten, wurde der Fokus zum Teil ausschließlich auf das methodische Vorgehen gelegt und keine inhaltliche Auswertung vorgenommen. Dies war insbesondere bei den DSFA der Fall. Für diese wurde nur bewertet, ob die dazu eingereichten Unterlagen zumindest die nach Art. 35 Abs. 7 DS-GVO geforderten Inhalte enthalten. So wurde zum Beispiel geprüft, ob eine Einstufung der Risikoschwere stattfand und diese begründet wurde. Es wurde dagegen nicht geprüft, ob die konkrete Einstufung von meiner Behörde für richtig gehalten wird. Eine detaillierte inhaltliche Prüfung hätte den für die Querschnittsprüfung kalkulierten zeitlichen Prüfungsrahmen bei knapp 200 vorgelegten DSFA weit überschritten.

In der Auswertung der Antworten wurde jedem Fragenkomplex eine Ampelfarbe zugeordnet, die zeigte, ob in diesem Bereich kein bzw. kaum (grün), normaler (gelb) oder erheblicher Handlungsbedarf (rot) herrschte. Ausgehend von den einzelnen Ergebnissen der zehn Komplexe erhielt jedes Unternehmen eine Gesamtbewertung, ebenfalls in Rot, Gelb oder Grün.

Bewertung in Rot, Gelb oder Grün

Bewertungsmethodik

Unternehmen, die bei keinem der Fragenkomplexe mit Rot bewertet wurden, bekamen in der Gesamtbetrachtung ein Grün, Unternehmen, bei denen ein Fragenkomplex als Rot eingestuft wurde, wurden insgesamt mit Gelb bewertet. Sowohl für die mit Grün als auch für die mit Gelb bewerteten Unternehmen war die Querschnittsprüfung mit Mitteilung des Prüfungsergebnisses beendet. Die „gelben" Unternehmen erhielten zusammen mit dem Prüfungsergebnis weitergehende Erläuterungen zum mit Rot bewerteten Fragenkomplex sowie den nachdrücklichen Hinweis, dass meine Behörde davon ausgeht, dass die Defizite zeitnah abgestellt werden.

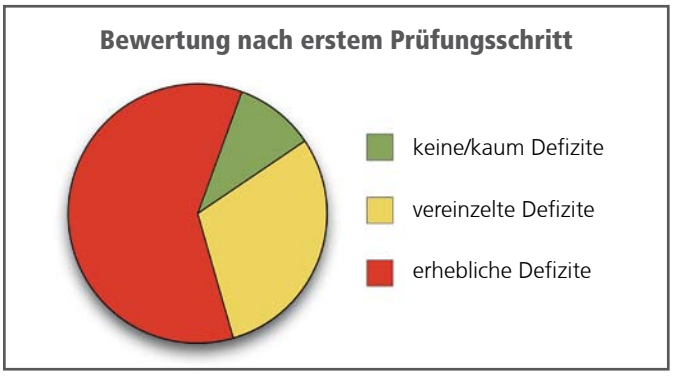
Zweiter Prüfungsschritt für „rote" Unternehmen

Unternehmen, die in mehr als einem Fragenkomplex mit Rot bewertet wurden, bekamen nach Mitteilung der Prüfungsergebnisse die Gelegenheit, zum Ergebnis Stellung zu nehmen und weitere Unterlagen einzureichen. Diese wurden geprüft und die Unternehmen anschließend erneut bewertet. Am Ende dieses zweiten Prüfungsschrittes wurde für alle Unternehmen die Querschnittsprüfung beendet. Unternehmen, die nun immer noch auf Rot standen, wurden allerdings darüber informiert, dass bei ihnen weiterhin gravierende Defizite zu erkennen sind. Weitergehende Kontrollen in separaten Prüfungen wurden angekündigt.

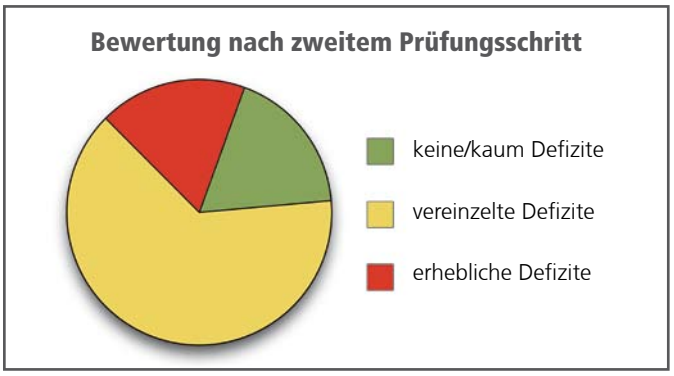
Ergebnisse: Neun Unternehmen bleiben rot

21 können sich verbessern

Nur 5 der geprüften 50 Unternehmen erhielten am Ende des ersten Prüfungsschrittes eine grüne Bewertung, d.h., nur bei diesen wurde in keinem der 10 Fragenkomplexe ein erheblicher Handlungsbedarf festgestellt. 15 Unternehmen erhielten Gelb als Bewertung, hatten also in einem der Fragenkomplexe erheblichen Handlungsbedarf. Auffällig war hier, dass dieser eine mit Rot bewertete Fragenkomplex entweder den technisch-organisatorischen Datenschutz oder die Datenschutz-Folgenabschätzung betraf. Bei 30 Unternehmen wurde in mehr als einem Fragenkomplex erheblicher Handlungsbedarf festgestellt, sie wurden also mit Rot bewertet. Jedes dieser 30 Unternehmen hatte erhebliche Defizite im technisch-organisatorischen Datenschutz und 25 von 30 auch bei der DSFA. In diesen beiden Bereichen zeigten sich bei den geprüften Unternehmen somit die mit Abstand größten Schwierigkeiten.



Im Zuge des zweiten Prüfungsschrittes konnten sich 4 der 30 Unternehmen von Rot auf Grün verbessern. 17 Unternehmen verbesserten sich auf insgesamt Gelb. Bei neun Unternehmen blieb es bei Rot als Gesamtbewertung. Als Endergebnis erhielten damit 9 Unternehmen das Prädikat „Grün", 32 „Gelb" und 9 „Rot".



Was funktioniert, was nicht?

In den Komplexen der Auftragsverarbeitungsverträge, der Datenschutzbeauftragten (DSB), der Meldepflichten und der Dokumentation stellte meine Behörde nur gelegentlich Defizite fest. Für die Auftragsverarbeitungsverträge wurden z. B. teilweise Muster verwendet, die nicht vollumfänglich der Rechtsauffassung der Aufsichtsbehörden entsprachen. Für die DSB wurde nicht immer deren Fachkunde ausreichend nachgewiesen. Bei den Meldeprozessen war zum Teil die Darstellung nicht vollständig nachvollziehbar, es fehlte teilweise eine klare Regelung der Verantwortlichkeiten oder eine eindeutige Berücksichtigung der 72-Stunden-Frist.

Häufiger lagen Defizite bei den Verzeichnissen von Verarbeitungstätigkeiten (VVT), den Einwilligungen sowie den Betroffenenrechten vor. So war beim VVT teilweise der unklar, wie das Verzeichnis aktualisiert wird. Zudem konnten Standardverfahren nicht erkannt werden (z. B. für das Betreiben der Webseite oder für das Bewerbungsverfahren) und Kontaktangaben fehlten. Einwilligungserklärungen waren ebenfalls bisweilen unklar: Es fehlten differenzierte Auswahlmöglichkeiten sowie Angaben, wo und wie ein Widerruf erfolgen kann. Hinsichtlich der Informationspflichten war ein Einsatz von Mustern erkennbar, ohne dass diese individuell an das jeweilige Unternehmen angepasst wurden.

Muster müssen individuell angepasst werden

Bei den Themen technisch-organisatorischer Datenschutz und DSFA lagen bei den Antworten verbreitet erhebliche Defizite vor. Beim technischen Datenschutz wurden Begrifflichkeiten wie z. B. der „Stand der Technik" ganz überwiegend nicht richtig verstanden. Die Konzepte Privacy by Design bzw. by Default scheinen mehrheitlich noch wenig vertraut zu sein. In einigen Branchen wurde bei der Einschätzung der Risiken zudem der Fokus auf die (finanziellen) Risiken für das Unternehmen gelegt. Die Unternehmen trugen damit nicht der Tatsache Rechnung, dass beim Datenschutz der Fokus auf die Risiken für die Betroffenen zu legen ist. In Bezug auf die DSFA war vor allem problematisch, dass bei der Schwellwertprüfung verbreitet keine systematische Herangehensweise erkennbar war.

Fokus auf den eigenen Interessen, nicht auf Betroffenen

Schlussfolgerungen

Aus der Querschnittsprüfung haben sich für meine Behörde Erkenntnisse ergeben, die sowohl die Vollzugsaufgaben berühren als auch die Pflicht zu Aufklärung und Sensibilisierung der Verantwortlichen.

Was den Vollzug betrifft, so war die Prüfung zwar auch für die Unternehmen beendet, die am Ende immer noch mit Rot bewertet worden waren. Allerdings wurden fünf von Ihnen mit der Mitteilung des Ergebnisses gleichzeitig darüber informiert, dass bei ihnen aufgrund der gravierenden Defizite weitergehende Kontrollen in separaten Prüfungen folgen werden. Über diese werde ich in meinem Tätigkeitsbericht für das Jahr 2020 informieren. Nicht auszuschließen ist, dass ich in Folge dieser Kontrollen auch Bußgelder verhängen werde. Dabei wird meine Behörde u.a. berücksichtigen, wie schwerwiegend ein möglicherweise vorliegender Verstoß ist und wie das Unternehmen damit umgegangen ist.

Separate Prüfungen bei fünf Unternehmen

Zudem plane ich, verstärkt weitere themen- und branchenbezogene anlasslose Kontrollen durchzuführen.

Weitere Informationsangebote in Arbeit

Zugleich werde ich den eingeschlagenen Weg fortsetzen, das Beratungs- und Informationsangebot auf meiner Webseite an die identifizierten Bedarfe anzupassen. Die Querschnittsprüfung hat sehr deutlich gezeigt, dass die größten Schwierigkeiten in der Umsetzung der DS-GVO in den Bereichen technisch-organisatorischer Datenschutz und DSFA liegen. Deshalb habe ich beschlossen, Handlungsempfehlungen zu den Themen „Stand der Technik", „Rollen- und Berechtigungskonzepte", „Privacy by Design und by Default" sowie zur Schwellwertprüfung bei der DSFA zu veröffentlichen. Darüber hinaus wird es auch eine Handlungsempfehlung für Einwilligungserklärungen geben.

Im Rahmen der Querschnittsprüfung ist teilweise der Eindruck entstanden, dass Unternehmen selbst die Tatbestandsvoraussetzungen nicht hinreichend berücksichtigt haben, die sich aus den jeweiligen Normen klar ergeben. Bei zukünftigen Prüfungen müssen die Unternehmen sich mit den gesetzlichen Anforderungen vertieft auseinandersetzen, diese auf ihre individuelle Situation übertragen und umsetzen. Die daraus resultierenden Prozesse sollten eine (nachvollziehbare) Methodik aufweisen, die sicherstellt, dass die gesetzlichen Anforderungen im Einzelfall erfüllt werden.

6.2 Automatisierte Fahrzeuge datenschutzkonform entwickeln

Die Weiterentwicklung des autonomen Fahrens ist eine große Herausforderung für die Abwägung zwischen den berechtigten Interessen der Bürger und dem Innovationsdruck in der Automobil-Industrie. Entwicklungsfahrten und die damit verbundenen Aufzeichnungen sind dabei von besonderer Bedeutung. Meine Behörde beteiligt sich an einem Arbeitskreis, der die Anforderungen der DS-GVO auf diesem Feld präzisieren möchte.

Für die Entwicklung automatisierter Fahrzeuge werden Entwicklungsfahrten durchgeführt, bei denen Bildaufnahmen gemacht werden. Diese Fahrten finden sowohl auf Teststrecken, die unter anderem auch in Niedersachsen eingerichtet wurden, als auch im öffentlichen Raum statt. Zwar hat grundsätzlich jeder Mensch das Recht, sich in der Öffentlichkeit zu bewegen, ohne dabei beobachtet oder gar aufgezeichnet zu werden. Art. 6 Abs. 1 lit. f der Datenschutz-Grundverordnung (DS-GVO) kann die Verarbeitung dieser Bildaufnahmen jedoch rechtfertigen, sofern die Voraussetzungen dafür und weitere datenschutzrechtliche Anforderungen erfüllt werden.

Sensoren müssen Umfeld korrekt erfassen

Die Entwicklung automatisierter Fahrzeuge ist mit der Hoffnung auf einen umweltfreundlichen, flüssigen und sicheren Verkehr verbunden. Damit sich ein Fahrzeug automatisiert durch den Straßenverkehr bewegen kann, muss sein Umfeld korrekt von Sensoren erfasst und anschließend klassifiziert werden. Es könnte – und ist in der Vergangenheit bereits geschehen – zu fatalen Unfällen kommen, wenn z. B. ein Fußgänger nicht als solcher erkannt würde.

Selbstlernende Systeme brauchen Training

Die Klassifizierung von Objekten wird regelmäßig von selbstlernenden Systemen durchgeführt. Um diese Systeme zu ertüchtigen, sind Trainingsdaten erforderlich, die authentisch Situationen abbilden, mit welchen die Systeme dann auch im Echteinsatz konfrontiert sind. Daher planen u.a. Autobauer, Zulieferer und Universitäten Entwicklungsfahrten mit Testfahrzeugen, bei denen Kameras Bildmaterial gewinnen, welches dann für das Training der selbstlernenden Systeme genutzt wird.

Rechtsgrundlagen für Entwicklungsfahrten

Einwilligung und Vertrag kommen nicht in Frage

Datenschutzrechtlich betrachtet kann es sich bei diesen Aufnahmen um eine Erhebung personenbezogener Daten handeln, wenn auf den Bildern Personen oder personenbezogene Daten, wie z. B. Autokennzeichen, erkennbar sind. Es bedarf also einer Rechtsgrundlage für deren Verarbeitung. Wenig praktikabel

wäre es, zu versuchen, von allen anderen betroffenen Verkehrsteilnehmern eine Einwilligung einzuholen. Es existieren zwischen den betroffenen Personen und dem Verantwortlichen im Regelfall auch keine Vertragsbeziehungen, sodass die Verarbeitung nicht auf eine Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO gestützt werden kann. Sie dient auch nicht der Erfüllung eines Vertrages mit dem Betroffenen gem. Art. 6 Abs. 1 lit. b DSGVO.

Als Rechtsgrundlage kommt demnach bei nicht-öffentlichen Stellen Art. 6 Abs. 1 lit. f DS-GVO in Betracht, es hat also eine Abwägung zwischen den Interessen des Verantwortlichen und den Interessen, Grundrechten und Grundfreiheiten der betroffenen Personen stattzufinden. Wenn sich Verantwortliche auf diese Grundlage berufen, bedarf es stets einer Abwägung im Einzelfall. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat im März 2019 eine Orientierungshilfe für Anbieter von Telemedien veröffentlicht, in der umfassend die Voraussetzungen dieser Rechtsgrundlage und die bei der Abwägung zu beachtenden Kriterien erläutert werden. Diese Erläuterungen lassen sich auf andere Sachverhalte abseits von Telemedien übertragen und können auch für die Beurteilung der datenschutzrechtlichen Zulässigkeit von Entwicklungsfahrten entsprechend angewendet werden.

Orientierungshilfe https://t1p.de/oh-telemedien

Große Bedeutung von Forschung und Entwicklung

Wendet man Art. 6 Abs. 1 lit. f DS-GVO auf Entwicklungsfahrten an, können insbesondere folgende Aspekte eine große Rolle spielen:

- Eine Verpixelung von Gesichtern und Autokennzeichen würde dazu führen, dass die mit den verfälschten Bildern trainierten Systeme nicht mit den unverfälschten Sensordaten des Fahrzeugs im Echtbetrieb funktionieren würden. Es ist daher erforderlich, dass unverfälschte Bilddaten genutzt werden.
- Der Verordnungsgeber hat wissenschaftlicher Forschung und technischer Entwicklung ein hohes Gewicht eingeräumt, z. B. in Art. 89 und EG 159 DS-GVO.
- Es findet lediglich eine kurzzeitige Erfassung von Personen im öffentlichen Raum und keine Identifizierung statt.

Neben der Prüfung der Rechtsgrundlage sind natürlich noch weitere datenschutzrechtliche Anforderungen zu beachten: so z. B. die Erfüllung der Informationspflichten durch Kennzeichnung der Fahrzeuge, die Durchführung einer Datenschutz-Folgenabschätzung und die Implementierung von angemessenen technischen und organisatorischen Schutzmaßnahmen.

Fahrzeuge müssen gekennzeichnet werden

Daher hat 2019 ein Arbeitskreis der Aufsichtsbehörden unter meiner Beteiligung begonnen, mit dem Verband der Automobilindustrie Gespräche zu diesem Thema zu führen. Ziel ist es, die Anforderungen der DS-GVO für Entwicklungsfahrten zu präzisieren. Der Arbeitskreis beabsichtigt, im Lauf des Jahres 2020 zu einer entsprechenden Vereinbarung zu kommen.

6.3 Reklame ohne Ende – täglich grüßt die Werbeflut

Wenn es eine Hitliste der häufigsten Datenschutzbeschwerden gäbe, würden sie einen der vorderen Plätze belegen: Beschwerden über unverlangt zugesandte Werbung. Die Betroffenen fühlen sich von den ungewollten Postsendungen und E-Mails belästigt und fragen mich vielfach um Rat, wie sie diese Papier- und Newsletter-Flut eindämmen können.

Viele Betroffene nehmen an, Werbeansprachen wären nur dann datenschutzrechtlich zulässig, wenn sie dazu vorher ausdrücklich ihre Einwilligung gegeben haben. Das ist allerdings ein weit verbreiteter Irrtum. Tatsächlich verhält es sich so, dass E-Mail-Adressen, die unmittelbar von den betroffenen Personen im Rahmen einer Geschäftsbeziehung (Bestandskunden) erhoben wurden, grundsätzlich für Werbung genutzt werden können. Voraussetzung ist allerdings, dass dieser Zweck der E-Mail-Werbung entsprechend Art. 13 Abs. 1 lit c Datenschutz-Grundverordnung (DS-GVO) den betroffenen Personen bei der Datenerhebung transparent dargelegt worden ist.

Kunden müssen transparent informiert werden

Überwiegende schutzwürdige Interessen der betroffenen Person nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO sind insbesondere dann nicht gegeben, wenn die in § 7 Abs. 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) enthaltenen Vorgaben für elektronische Werbung eingehalten werden. So ist eine unzumutbare Belästigung durch E-Mail-Werbung nicht anzunehmen, wenn ein Unternehmer durch den Verkauf einer Ware oder Dienstleistung vom Kunden dessen E-Mail-Adresse erhalten hat und diese zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet. Das setzt voraus, dass der Kunde der Verwendung nicht widersprochen hat und bei Erhebung der Adresse sowie jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er jederzeit widersprechen kann.

Bestand allerdings bislang keine Geschäftsbeziehung mit dem Empfänger, dürfen E-Mail-Adressen nicht ohne Weiteres für Werbung bzw. den Newsletter-Versand verwendet werden. Dies ist nur erlaubt, wenn hierfür eine vorher ausdrücklich erklärte Einwilligung gegeben ist, egal ob Verbraucher (B2C – business to customer) oder Kontaktpartner in Unternehmen (B2B – business to business) angesprochen werden.

Postalische Werbung ohne Einwilligung

Mit Werbesendungen per Post verhält es sich ebenfalls so, dass diese zulässig sind, solange eine gesetzliche Legitimierung gemäß Art. 6 Abs. 1 lit. a – f DS-GVO vorliegt. Auch hier käme es also nicht explizit auf eine Einwilligung der Beschwerdeführenden an.

Dies gilt allerdings sowohl im Falle von elektronischer wie auch von postalischer Werbung nur, solange die Betroffenen keinen Gebrauch von ihrem Widerspruchsrecht gemäß Art. 21 Abs. 1 DS-GVO gemacht haben.

Händler und Makler für Adressen

Unternehmen erheben die Adressen in der Regel nicht selbst

Vielfach fragten mich Bürgerinnen und Bürger zudem, wie die werbetreibenden Unternehmen an ihre Adresse gekommen sind. In diesem Zusammenhang wurde etwa das zögerliche Verhalten der Unternehmen beanstandet, Auskunft über die Datenherkunft zu erteilen. Bei der Auseinandersetzung mit diesen Beschwerden ist mir jedoch aufgefallen, dass vielfach noch unklar ist, dass die werbetreibenden Unternehmen meist gar nicht für den Versand des Werbematerials verantwortlich sind.

So erheben Unternehmen nicht selbst Adressdaten, sondern nehmen die Dienste von Adresshändlern in Anspruch. Letztere übermitteln die Daten an einen unbeteiligten Dienstleister, den sogenannten Listbroker (zu Deutsch: Adressmakler). Dieser versendet dann das Werbematerial des Unternehmens. Dabei erfolgt vor dem Versand ein Abgleich mit der Sperrliste des Unternehmens und der Robinsonliste[1], um zu verhindern, dass Personen, die der Werbung widersprochen haben, angeschrieben werden

Somit werden die Versandadressen dem werbenden Unternehmen zunächst nicht bekannt. Das Unternehmen erhält vielmehr erst dann Kenntnis von den Daten, wenn der oder die Angeschriebene ein Angebot anfordert, einen Vertrag abschließt oder beispielsweise der Werbung widerspricht.

Einzig und allein der Dienstleister kann daher Auskunft über die Herkunft der Adresse erteilen. Alle Werbematerialien enthalten eine Auskunft darüber, wer im Sinne der DS-GVO der verantwortliche Dienstleister ist beziehungsweise bei welchem Dienstleister Widerspruch nach Art. 21 DS-GVO eingelegt werden kann. Dies ermöglicht den Bürgerinnen und Bürgern, den Verantwortlichen zu kontaktieren und weiteren Zusendungen zu widersprechen.

Unterrichtungspflichten bei Werbung per Post

Verantwortlicher muss klar erkennbar sein

Die Anmietung von Adressen über Dienstleister ist datenschutzrechtlich grundsätzlich nicht zu beanstanden, solange das Werbematerial die gesetzlichen Informationspflichten berücksichtigt. So müssen der für die personenbezogenen Daten Verantwortliche, das werbende Unternehmen und die Quelle der Daten aus einer Werbung eindeutig hervorgehen und klar ersichtlich sein.

Bei der Auseinandersetzung mit diesen Beschwerden ist mir aufgefallen, dass bereits viele werbetreibende Unternehmen ihren Unterrichtungspflichten gegenüber den Angeschriebenen nachkommen. Gleichwohl gehe ich davon aus, dass sich meine Behörde auch zukünftig mit dem Thema befassen wird.

1 Die Robinsonliste der Werbewirtschaft ist eine Schutzliste, auf die sich Personen, die keine Werbung wünschen, eintragen können. So verhindern sie, dass sie mit Werbung angeschrieben werden (https://www.robinsonliste.de).

Ansonsten gilt: Erst wenn der Angeschriebene gegenüber der verantwortlichen Stelle Gebrauch von seinem Widerspruchsrecht gemäß Art. 21 Abs. 1 DS-GVO macht, werden zuvor zulässige(r) Adresshandel und Werbung unzulässig.

Löschung und Widerspruch

Trotz gelöschter Daten kann wieder Werbung kommen

Die mir vorliegenden Fälle zeigten, dass Bürgerinnen und Bürger häufig nicht ihren Widerspruch gegenüber der verantwortlichen Stelle geltend machen. Vielmehr verlangten viele lediglich die Löschung ihrer Adressdaten. Daraus ergibt sich folgendes Problem: Hat das Unternehmen wunschgemäß die Daten eines Betroffenen gelöscht, kann es trotzdem passieren, dass dieser wieder Werbung erhält. Nämlich dann, wenn das werbetreibende Unternehmen später Adressen kauft und die Daten wieder in den Adressbeständen enthalten sind.

Deshalb empfehle ich, von Unternehmen nicht nur die Löschung der Daten zu verlangen, sondern zusätzlich auch Widerspruch einzulegen. Denn dann muss die Adresse in eine Werbe-Sperrdatei aufgenommen werden. Dies ermöglicht die Überprüfung, ob zu den jeweils neu erworbenen Adressen bereits ein Widerspruch vorliegt.

6.4 Verhaltens- und Leistungskontrollen von Beschäftigten

Unternehmen haben ein Interesse daran, über die Arbeitsleistungen ihrer Beschäftigten im Bild zu sein. Dabei müssen sie sich allerdings an die gesetzlichen Bestimmungen zum Beschäftigtendatenschutz halten.

Ortung per GPS

Meine Behörde sah sich in den vergangenen Jahren immer wieder mit der GPS-Überwachung von Beschäftigten konfrontiert. Im Berichtszeitraum musste ich mich nun erneut mit einem Fall aus dem Jahr 2017 beschäftigen: Bei einem Kontrollverfahren sah meine Behörde es nicht als erforderlich an, dass ein GPS-Ortungssystem in Firmenfahrzeugen einer Gebäudeservice-Firma (Reinigungsgewerbe) eingesetzt wurde. Es kam dadurch zu unzulässigen Verarbeitungen von personenbezogenen Daten der Beschäftigten. Die Rechtswidrigkeit wurde in einem Bescheid festgestellt und der weitere Einsatz des GPS-Ortungssystems weitgehend untersagt. Er wurde allein für den Fall eines Diebstahls als zulässig bewertet, um das Fahrzeug wiederzufinden. Gegen diesen Bescheid hatte das Unternehmen Klage erhoben.

GPS-Ortung nur bei Diebstahl zulässig

Das Verwaltungsgericht (VG) Lüneburg bestätigte meine Entscheidung mit Urteil vom 15. März 2019, Aktenzeichen 4 A 12/19, und wies die Klage der Firma ab. Das Gericht hat sich ausführlich mit den möglichen Einsatzformen von GPS-Ortungssystemen im Beschäftigungsverhältnis auseinandergesetzt. Das Urteil enthält unter anderem Ausführungen zur Erforderlichkeit der Verarbeitung von Positionsdaten durch Arbeitgeber mithilfe von Ortungssystemen (zum Beispiel zur Tourenplanung, zum Diebstahlschutz und zur Nachweispflicht für die Abrechnung mit Kunden). Im Ergebnis wurde in diesem Fall die Erforderlichkeit zur Beschäftigtenkontrolle abgelehnt.
Als Prüfungsmaßstab wurden vom Gericht Datenschutz-Grundverordnung (DS-GVO) sowie die Regelung des § 26 Bundesdatenschutzgesetz (BDSG) berücksichtigt. Gegen dieses Urteil wurde jedoch beim Oberverwaltungsgericht Lüneburg unter dem Aktenzeichen 11 LA 154/19 Berufung eingelegt. Eine abschließende Entscheidung steht noch aus.

Zurechenbarkeit von Handlungen

Im Rahmen eines noch laufenden Klageverfahrens, bei dem es um die Standortüberwachung eines früheren Beschäftigten geht, stellte sich die Frage nach dem Verantwortlichen. Die Besonderheit des Falles ist, dass die Standortüberwachung vor Inkrafttreten der DS-GVO beendet wurde und somit materiellrechtlich am Maßstab des Bundesdatenschutzgesetzes alter Fassung (BDSG a. F.) zu messen war. Offen ist – im Hinblick auf die datenschutzrechtliche Ver-

antwortlichkeit –, ob die veranlasste Verarbeitung der Beschäftigtendaten im Rahmen einer „Funktionsübertragung" vom Tochterunternehmen an die Konzernmutter oder als Auftragsdatenverarbeitung nach § 11 BDSG a. F. durch die Konzernmutter durchgeführt wurde. Denn bei einer Funktionsübertragung wäre die Konzernmutter für die Verarbeitung verantwortlich.

Zur Abgrenzung einer weisungsgebundenen Datenverarbeitung im Auftrag nach § 11 BDSG a. F. von der im Gesetz nicht ausdrücklich geregelten sogenannten Funktionsübertragung ist maßgeblich, ob der Dienstleister lediglich zur Erbringung untergeordneter Hilfsdienste ohne eigenen Wertungs- und Entscheidungsspielraum eingebunden wird oder ob er insbesondere eigene materielle vertragliche Leistungen über die technische Datenverarbeitung hinaus erbringt.

Nur Hilfsdienste oder eigene Leistungen?

Speziell für die Fälle zentralisierter (Konzern-)Personalabteilungen wird die Funktionsübertragung grundsätzlich als zulässig angesehen. Eine endgültige Bewertung ist jedoch nur anhand einer Einzelfallbetrachtung möglich. Hierbei sind die konkret zwischen den Parteien vereinbarten Bedingungen der Zusammenarbeit entscheidend.

Die entsprechende Auswertung der vertraglichen Regelungen durch meine Behörde hat ergeben, dass eine Datenverarbeitung im Auftrag vorgelegen hat. Es bestand in den entscheidungsrelevanten Bereichen eine Weisungsabhängigkeit der Konzernmutter von der Tochter. In Folge dessen blieb es bei der Verantwortlichkeit des Tochterunternehmens. Das Ergebnis des zum Ende des Berichtszeitraums noch laufenden Verfahrens beim Verwaltungsgericht Hannover bleibt abzuwarten.

Videokameras und Handscanner

Meine Behörde hat im Jahr 2019 eine Datenschutzüberprüfung bei einem Logistikunternehmen mit Sitz in Niedersachsen eingeleitet. Durch die Kontrolle soll geklärt werden, ob die Vorgaben der DS-GVO eingehalten werden und ob die dort unter dem Stichwort „Feedback-Verfahren" vorgenommenen Datenverarbeitungen zu einer ständigen Verhaltens- und Leistungskontrolle der Beschäftigten führen.

Prüfung zum „Feedback-Verfahren"

Das Unternehmen wurde unter anderem um Stellungnahme gebeten, zu welchem Zweck und aufgrund welcher Rechtsgrundlage dort technische Hilfsmittel wie Videokameras und sogenannte Handscanner eingesetzt werden, ob diese geeignet sind, die Beschäftigten zu überwachen und deren Arbeitsverhalten zu bewerten und ob eine Datenschutz-Folgenabschätzung für die Verarbeitungsvorgänge vorliegt. Zudem werden Datenübermittlungen in andere EU-Länder sowie in Drittländer überprüft. Das Kontrollverfahren war zum Ende des Berichtszeitraums noch nicht abgeschlossen.

6.5 Telearbeit und mobiles Arbeiten

Sowohl in der Wirtschaft als auch in der öffentlichen Verwaltung werden Telearbeit und mobiles Arbeiten genutzt. Beschäftigte können – je nach Angebot und Vereinbarung – Anteile ihrer Arbeitsleistung ortsunabhängig erbringen. Datenschutzrechtliche Vorschriften stehen der Einrichtung von Telearbeitsplätzen oder dem mobilen Arbeiten grundsätzlich nicht entgegen.

Der Arbeitgeber oder Dienstherr ist Verantwortlicher im Sinne von Artikel 4 Nummer 7 der Datenschutz-Grundverordnung (DS-GVO). Das heißt, er ist dafür verantwortlich, dass die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden (insbesondere Art. 5 Abs. 1 DS-GVO). Hierzu besteht eine Rechenschaftspflicht.

Gefahren und Risiken

Auf aktuelle Systeme und Updates achten

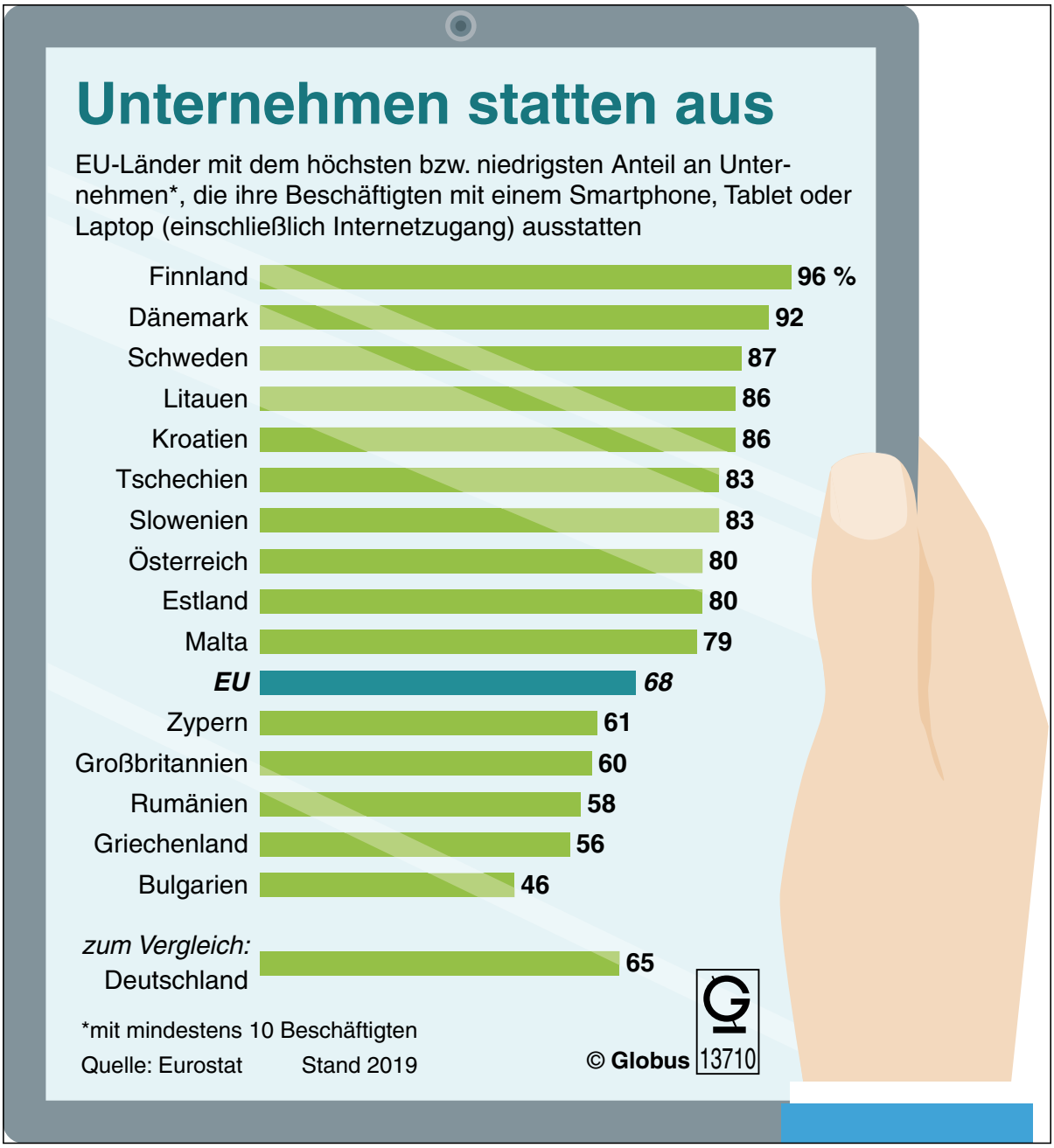
Verantwortliche und Auftragsverarbeiter müssen beachten, dass die genannten Angebote besondere Gefahren und Risiken bergen. Häufig sind mobile Endgeräte nicht hinreichend abgesichert, werden mit veralteten Systemen betrieben oder mit inaktuellen Sicherheitsupdates. Sie stellen ein Einfallstor für den Zugriff unbefugter Personen auf sensible Daten wie Zugangs- und Zugriffsberechtigungen dar. Auch weitere technische Schwachstellen, wie zum Beispiel die Nutzung von offenen WLAN-Verbindungen, müssen vermieden werden.

Verantwortliche müssen sich – ausgerichtet am Schutzbedarf der auf mobilen Arbeitsplätzen verarbeiteten Daten – mit diesen Gefahren und Risiken auseinandersetzen (siehe hierzu insbesondere Art. 24 Abs. 1, 25 Abs. 1 und 32 Abs. 1 DS-GVO). Bei voraussichtlich hohen Risiken muss eine Datenschutz-Folgenabschätzung erstellt werden (Art. 35 Abs. 1 DS-GVO). Je nach Ausgestaltung des konkreten Arbeitsplatzes müssen geeignete technische und organisatorische Sicherungsmaßnahmen ergriffen werden, um ein angemessenes Schutzniveau zu erreichen. Zum Nachweis stehen sowohl der Verantwortliche als auch der Auftragsverarbeiter in der Pflicht, diese Maßnahmen in regelmäßig zu evaluierenden Sicherheitskonzepten zu dokumentieren (Art. 32 Abs Satz 1 lit. d und Art. 5 Abs. 2 DS-GVO).

Kontrollen zu Hause erlaubt?

Grundgesetzt garantiert Unverletzlichkeit der Wohnung

Im Berichtszeitraum erreichten mich Anfragen, ob der Verantwortliche, der Auftragsverarbeiter, deren Datenschutzbeauftragte (DSB) oder die Datenschutzaufsichtsbehörde im Rahmen der ihnen obliegenden Kontrollaufgaben private Wohnungen von Telearbeitenden betreten dürfen („Betretungsrecht").



Artikel 13 des Grundgesetzes (GG) garantiert die Unverletzlichkeit der Wohnung. Die Grundrechte sind als objektive Wertordnung sowohl vom Verantwortlichen und dem Auftragsverarbeiter als auch vom DSB und der Aufsichtsbehörde zu beachten, so dass Artikel 13 GG Beschäftigten jedenfalls mittelbar Schutz gewährt. Es besteht damit ein Spannungsverhältnis, wenn gleichzeitig Kontrollaufgaben wahrgenommen werden sollen.

Der Verantwortliche hat nicht nur das Recht, sondern auch die Pflicht, vor und nach der Genehmigung von Telearbeit routinemäßig und in regelmäßigen Abständen zu kontrollieren, ob die Beschäftigten die datenschutzrechtlichen Vorgaben einhalten. Dies gilt vor allem, wenn bei Telearbeit besonders schutzwürdige personenbezogene Daten verarbeitet werden. In diesem Zusammenhang muss der Verantwortliche bei Telearbeitsplätzen Zugang zur Wohnung des Beschäftigten haben.

Zutrittsrecht vertraglich vereinbaren

Aufgrund der Bedeutung des Artikels 13 GG kann in der Vereinbarung von Telearbeit aber nicht eine stillschweigende Zustimmung zum Betreten der Wohnung angenommen werden. Das notwendige Zutrittsrecht des Arbeitgebers oder beauftragter Personen muss daher vertraglich mit dem Beschäftigten vereinbart werden. Davon muss auch das Einverständnis der mit dem Beschäftigten in häuslicher Gemeinschaft zusammenlebenden Personen umfasst sein. Der DSB ist aufgrund der Regelung in Art. 38 Abs. 2 DS-GVO in das vertraglich ausgestaltete Zutrittsrecht einzubeziehen.

Befugnisse der Aufsichtsbehörde

Die Datenschutzaufsichtsbehörden verfügen nach Art. 58 Abs. 1 der DS-GVO über umfangreiche Untersuchungsbefugnisse. Hierzu zählt auch das Recht zum Zugang zum Grundstück und zu den Geschäfts- oder Diensträumen des Verantwortlichen und des Auftragsverarbeiters. Bezogen auf den Wortlaut ist der Zugang auf Grundstücke und Geschäfts- oder Diensträume beschränkt. Die Privaträume der Beschäftigten sind hiervon ausgenommen.

Grundsatz der Verhältnismäßigkeit

Bei der Ausübung der Kontroll-Befugnisse muss die Aufsichtsbehörde den Grundsatz der Verhältnismäßigkeit beachten, sofern mit der Ausübung dieser Befugnisse Eingriffe in die Grundrechte der Betroffenen verbunden sind. Nach Erwägungsgrund 129 sollte jede Maßnahme zur Einhaltung der DS-GVO geeignet, erforderlich und verhältnismäßig sein, wobei unter anderem die Umstände des Einzelfalls zu berücksichtigen sind.

Sofern es sich um „Dienst-/Geschäftsräume" im Rahmen der Telearbeit in Privatwohnungen der Beschäftigten handelt, muss der Verantwortliche dafür Sorge tragen, dass die Aufsichtsbehörde Zugang erhält. Sofern der Aufsichtsbehörde der Zugang durch die Beschäftigten verwehrt wird, muss der Verantwortliche auf andere angemessene Weise seiner Rechenschaftspflicht nachkommen. Gleiches gilt für den Verantwortlichen im Fall der Auftragsdatenverarbeitung.

Der Verantwortliche ist zum Nachweis verpflichtet, dass er die Grundsätze für die Verarbeitung personenbezogener Daten einhält. Sollte er seiner Rechenschaftspflicht wegen der Zutrittsverweigerung seiner Beschäftigten nicht nachkommen können, muss er den datenschutzrechtlichen Verstoß verantworten.

Ich empfehle deshalb, die Gewährung von Telearbeit stets von der Einwilligung der Beschäftigten zum „Betretungsrecht" abhängig zu machen. In einen Auftragsverarbeitungsvertrag wäre eine entsprechende vertragliche Verpflichtung des Auftragsverarbeiters im Sinne des Art. 28 Abs. 1 DS-GVO aufzunehmen.

J.7. Gesundheit

7.1 Neu in Niedersachsen: Runder Tisch im Gesundheitswesen

Der Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 hat die Sensibilität von Patienten für ihre Gesundheitsdaten erhöht. Gleichzeitig stieg der Beratungsbedarf von Ärzten, Zahnärzten und Apothekern. Ich habe deshalb mit den maßgeblichen Akteuren einen „Runden Tisch im Gesundheitswesen" ins Leben gerufen.

Gesundheitsdaten gehören zu den Kategorien besonders sensibler Daten gem. Art. 9 Abs. 1 DS-GVO. Deshalb war es keine Überraschung, dass sich zum Geltungsbeginn der Verordnung großer Beratungsbedarf in diesem Bereich zeigte.

Die im Juli 2018 veröffentlichten FAQ im Gesundheitswesen beantworten bereits viele Fragen und werden regelmäßig ergänzt. An verschiedenen Beratungsanfragen wurde jedoch deutlich, dass trotz der Verteilung an die jeweiligen Interessenvertretungen nicht alle Verantwortlichen im Gesundheitsbereich Kenntnis von den FAQ hatten.

FAQ Gesundheitswesen: https://t1p.de/faq-gesundheit

Gespräche mit den jeweiligen Kammern und Interessensvertretungen ergaben, dass auch an sie in vielen Fällen ähnliche Fragen herangetragen werden. Um ein in Niedersachsen einheitlich hohes Datenschutzniveau zu erreichen, ist aus meiner Sicht eine gute Vernetzung der Akteure mit meiner Behörde sowie untereinander wünschenswert.

Aufgaben und Inhalte des Runden Tisches

Aus diesem Grund habe ich mit der Ärztekammer, der Zahnärztekammer, der Kassenärztlichen Vereinigung, der Kassenzahnärztlichen Vereinigung, der Apothekerkammer sowie dem Psychotherapeutenverband den „Runden Tisch im Gesundheitswesen" initiiert. Im Fokus des Netzwerks steht der Informationsaustausch auf Arbeitsebene.

Fragen zu Betroffenenrechten

Die Teilnehmer des Runden Tischs trafen sich erstmals am 13. Mai 2019. Auf Seiten der Interessenvertreter waren nach wie vor grundlegende Themen wie

die Vorgaben zu Auskunfts- und Informationspflichten sowie zu Einwilligungen von großem Interesse. Von Seiten der Aufsichtsbehörden informierte ich die Runde über die aktuellen Arbeiten der Datenschutzkonferenz am Whitepaper zum Einsatz von Messenger-Diensten in Krankenhäusern (siehe hierzu auch Seite 161).

Für die Zukunft ist es das erklärte Ziel aller Beteiligten, zweimal jährlich, jeweils nach den Hauptsitzungen der Datenschutzkonferenz zu einem Austausch zusammenzukommen.

7.2 Prüfung zur Umsetzung der DS-GVO in Krankenhäusern

Wie in meinem 24. Tätigkeitsbericht angekündigt habe ich die Umsetzung der Datenschutz-Grundverordnung (DS-GVO) in drei zufällig ausgewählten niedersächsischen Krankenhäusern geprüft. Dabei fragte ich auch ab, inwieweit die Krankenhäuser die Orientierungshilfe zu Krankenhausinformationssystemen nutzen.

Mein Fragebogen umfasste 15 Fragen zum allgemeinen Datenschutzrecht, zu den Betroffenenrechten und zur Orientierungshilfe Krankenhausinformationssysteme (OH-KIS). Aufgrund der geringen Zahl der geprüften Krankenhäuser ist das Ergebnis der Auswertung nicht repräsentativ. Zunächst sollte nur ein Überblick erzielt werden, in welchen Bereichen eine tiefergehende Prüfung sinnvoll ist.

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

Krankenhäuser sind allgemein gut aufgestellt

Die Auswertung ergab, dass die geprüften Krankenhäuser im Bereich der allgemeinen Fragen zum Datenschutz gut aufgestellt sind. Jede Einrichtung hatte einen Datenschutzbeauftragten (DSB) benannt und alle Beschäftigten werden mindestens einmal jährlich datenschutzrechtlich geschult. In allen Einrichtungen liegt zudem ein Verzeichnis der Verarbeitungstätigkeiten vor. Der Meldeweg für eine Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO ist ebenso in Verfahrensanweisungen festgelegt, wie die Erteilung einer Auskunft nach Art. 15 DS-GVO.

Zu wenig Zeit für Datenschutzbeauftragte

Die datenschutzrechtlichen Handlungsfelder in den Krankenhäusern sind vielfältig. Die betrieblichen DSB vor Ort müssen die Einhaltung des Datenschutzes gegenüber den Beschäftigten genauso kontrollieren wie den Schutz der Patientendaten. Dies setzt nicht nur umfangreiche Kenntnisse im Datenschutzrecht voraus, sondern auch ausreichende Zeitanteile bzw. eine ausreichende Anzahl an Beschäftigten, welche den DSB, nicht nur während des Urlaubs oder bei Abwesenheit, vertreten und unterstützen. Die verspätete Meldung einer Datenpanne, nur weil der DSB nicht erreichbar gewesen ist, wird von mir nicht toleriert.

Benennung von DSB im Gesundheitswesen: https://t1p.de/Benennung-DSB-Gesundheitswesen

Zwar sehen die Datenschutzgesetze keine gesetzliche Pflicht zur Freistellung von DSB vor. Dennoch sollte jedem Verantwortlichen bewusst sein, dass in einem Krankenhaus mittlerer Größe mit mehreren Dutzend Beschäftigten und Tausenden von Patienten pro Jahr mindestens eine Vollzeitstelle für den Datenschutz eingeplant werden muss.

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

Betroffenenrechte werden erfüllt

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 nun auch ein umfassender datenschutzrechtlicher Auskunftsanspruch zugestanden. Für die fristgemäße Umsetzung von Auskunftsersuchen gibt es in den geprüften Häusern entsprechende Verfahrensanweisungen.

Patienten müssen vorab informiert werden

Dennoch bringt die DS-GVO auch in diesem Bereich Neuerungen mit sich. Auch die Patienten eines Krankenhauses müssen vor Beginn der Verarbeitung ihrer personenbezogenen Daten über die Art und Weise der Verarbeitung informiert werden.

Bei der Umsetzung der Betroffenenrechte nach den Artikeln 12 ff. DS-GVO haben sich keine Beanstandungen ergeben. Die vorgeschriebenen Informationen werden den Patientinnen und Patienten vor Beginn der Behandlung zugänglich gemacht.

Orientierungshilfe Informationssysteme

Der Datenschutz im Gesundheitswesen war in Deutschland bereits vor der DS-GVO auf einem sehr hohen Niveau. Für Krankenhäuser gibt es seit einigen Jahren bereits eine von den Datenschutzaufsichtsbehörden entwickelte Orientierungshilfe Krankenhausinformationssysteme, welche die rechtlichen Auslegungen der Aufsichtsbehörden zu den Datenschutzvorschriften formuliert. Diese Orientierungshilfe behält auch mit der DS-GVO ihre Gültigkeit.

Bei der Umsetzung der OH KIS scheint noch Verbesserungspotenzial in den Krankenhäusern zu bestehen. Obgleich nur ein kleiner Auszug abgefragt wurde, offenbaren sich Schwächen bei der Umsetzung der Rollen- und Rechtekonzepte, wenn es um die Zugriffsrechte für Ärzte geht. Eine regelmäßige Protokollierung und anlassunabhängige Auswertung der Zugriffe auf Patientenakten kann ebenso verbessert werden, wie die in Art. 18 DS-GVO vorgesehene Einschränkung der Verarbeitung abgeschlossener Fälle.

Ausweitung der Prüfung geplant

Mit der durchgeführten Prüfung konnte bereits ein guter Überblick gewonnen werden, in welchen Bereichen eine weitergehende Prüfung sinnvoll ist. Ich beabsichtige daher ab dem Jahr 2020 eine Vielzahl von Krankenhäusern zu überprüfen.

1 1 §§ 630a ff. BGB

7.3 Anforderungen an Messenger in Krankenhäusern

Messenger-Dienste sind im privaten Bereich längst etabliert. Zunehmend kommen diese Anwendungen inzwischen auch in Krankenhäusern zum Einsatz – häufig auf privaten Endgeräten. Jedoch sind längst nicht alle Anwendungen datenschutzkonform. Deshalb wurde unter der Federführung des Datenschutzbeauftragten von Rheinland-Pfalz und meiner Behörde ein Whitepaper zu Messengern im Krankenhausbereich erarbeitet.

Aufgrund der Sensibilität von Gesundheitsdaten ist es unabdingbar, dass Datenschutzstandards eingehalten werden. In der Praxis offenbaren sich zwei große datenschutzrechtliche Probleme: Unzureichend geschützte Endgeräte und datenschutzrechtlich unsichere Messenger-Dienste. Beide Aspekte greift das von der Datenschutzkonferenz (DSK) veröffentlichte Whitepaper „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich" auf.

Was ist ein Whitepaper?
Der Begriff „Whitepaper" ist die heute gebräuchliche Variante des ursprünglichen Begriffs des politischen Weißbuchs. Es ist ein Instrument der Öffentlichkeitsarbeit, das eine wertungsfreie, fachliche Übersicht über Leistungen, Standards und Technik, vor allem zu IT-Themen gibt.

Whitepaper Messenger-Dienste: https://t1p.de/messenger-kh

Sichere Endgeräte

Sofern besondere Kategorien personenbezogener Daten von Dritten, hier Patientendaten, auf mobilen Endgeräten verarbeitet werden sollen, müssen diese Geräte die Vorgaben des technisch-organisatorischen Datenschutzes erfüllen. Das Whitepaper formuliert die Mindestanforderungen an sichere Endgeräte. Verantwortliche oder deren Beschäftigte, die mobile Endgeräte im Krankenhausalltag nutzen, müssen darauf achten, diese Mindestanforderungen zu erfüllen, unabhängig davon, wer Eigentümer der Geräte ist.

Datenschutzgerechter Messenger

In der Praxis werden oft Messenger von Unternehmen eingesetzt, deren Firmensitz in einem Land außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung (DS-GVO) liegt. Diese Dienste übermitteln Daten ohne Rechtsgrundlage in Länder, in denen aufgrund der dortigen Gesetzeslage ein Zugriff auf die Daten nicht ausgeschlossen werden kann.

Kernforderungen: Verschlüsselung und Zugriffskontrolle

Das Whitepaper nennt die aus Sicht der Datenschutzaufsichtsbehörden technischen Anforderungen an Messenger-Dienste, die in Krankenhäusern eingesetzt werden können. Dies soll sowohl den Verantwortlichen im Krankenhaus, als auch den Herstellern von Messenger-Diensten helfen, eine für Gesundheitsdaten geeignete App auszuwählen bzw. zu programmieren.

Kernpunkte dieses Anforderungskatalogs sind die verschlüsselte Datenverarbeitung innerhalb der App und eine sichere Zugriffskontrolle auf die dort gespeicherten Daten.

Interessenvertreter eingebunden

In die Arbeit an dem Whitepaper wurden auch die Interessenvertreter der betroffenen Anwender eingebunden, etwa die Deutsche Krankenhausgesellschaft, die Bundesärztekammer, der Bundesverband Gesundheits-IT und der Verband der Krankenhausdirektoren Deutschlands. Nicht alle Anforderungen, die die Datenschutzkonferenz formuliert hat, wurden vollumfänglich geteilt, die Entwicklung des Whitepapers wurde hingegen von allen Teilnehmenden begrüßt.
Die Unterarbeitsgruppe „Digitalisierung im Gesundheitswesen“ der Datenschutzkonferenz wird das Whitepaper fortentwickeln.

7.4 Verarbeitung und Löschung von Patientendaten

Mit der DS-GVO ist der Wunsch von Patienten nach Löschung von Gesundheitsdaten bei Ärzten und in Krankenhäusern stärker in den Fokus gerückt. Gleichzeitig sind Ärzte unsicher, ob und wenn ja, wann Daten gelöscht werden dürfen.

Arztpraxen und Krankenhäusern haben die Befugnis, besondere Kategorien personenbezogener Daten in Form der Patientendaten zu verarbeiten. Das ergibt sich aus Art. 9 Abs. 2 lit. h) DS-GVO in Verbindung mit dem schriftlich oder mündlich geschlossenen Behandlungsvertrag.

Einwilligung nur bei Weitergabe an Dritte

Eine weitergehende Einwilligung in die Datenverarbeitung oder Entbindung von der Schweigepflicht ist nur dann erforderlich, wenn der Arzt oder das Krankenhaus die Daten des Patienten an dritte Stellen übermitteln möchte, die bisher nicht in den Behandlungsvertrag eingebunden sind. Exemplarisch kommen hier die Datenübermittlung an den Hausarzt[1] zur Dokumentation ohne Weiterbehandlung oder die Übermittlung der Abrechnungsdaten[2] an ein externes Unternehmen oder eine privatärztliche Verrechnungsstelle in Betracht.

Einwilligung muss nachgewiesen werden können

Der Verantwortliche muss nachweisen können, dass diese Einwilligung vorliegt. Deshalb empfehle ich in diesen Fällen weiterhin die Schriftform zu wählen, auch wenn die DS-GVO oder die einschlägigen Fachgesetze dies nicht mehr explizit vorsehen.

Pflicht zur Dokumentation

Arztpraxen und Krankenhäuser sind verpflichtet, eine eigene medizinische Dokumentation zu führen. Diese Pflicht ergibt sich sowohl aus § 630f Abs. 1 BGB, als auch aus den entsprechenden Vorschriften der einschlägigen Berufsordnungen. Behandlungsrelevante Unterlagen von Patienten oder Dritten können ebenso Teil der Dokumentation werden wie die eigenen Aufzeichnungen.

1 § 73 Abs. 1b SGB V

2 § 12 Abs. 2 Musterberufsordnung der Bundesärztekammer

Die Aufzeichnungen unterliegen verschiedenen Aufbewahrungsfristen.

Mindestens zehn Jahre aufbewahren

Nach § 630f Abs. 3 BGB sind Patientendaten immer mindestens zehn Jahre nach Abschluss der Behandlung aufzubewahren. Das Strahlenschutzgesetz[3] sieht für bestimmte Daten, wie beispielsweise Aufzeichnungen über Röntgenbehandlungen, sogar eine Mindestaufbewahrungsfrist von 30 Jahren vor.

Zur Abwehr von Schadensersatzansprüchen kann nach § 823 BGB in Verbindung mit § 199 Abs. 2 BGB in begründeten Fällen auch für andere Daten eine Aufbewahrungsfrist von 30 Jahren zulässig sein. Sofern eine Aufbewahrung nach Ablauf der gesetzlichen Frist im berechtigten Interesse des Patienten zu vermuten ist, dürfen die Daten ebenfalls länger aufbewahrt werden.

Fristen im VVT dokumentieren

Die Gründe und die Dauer der Datenspeicherung nach diesen Vorschriften sind von den Verantwortlichen im Verzeichnis der Verarbeitungstätigkeiten (VVT) darzulegen.

Die Fristen gelten unabhängig davon, auf welchem Medium die Patientendaten gespeichert werden. Eine Löschung vor Ablauf der Aufbewahrungspflicht ist nicht zulässig

Löschung von Daten

Pflicht zur Löschung vs. Pflicht zur Aufbewahrung

Art. 5 Abs. 1 lit. c) DS-GVO besagt, dass Daten nur so lange in einer Form, die die Identifizierung ermöglicht, gespeichert werden dürfen, wie es für die Zwecke der Datenverarbeitung erforderlich ist (Datensparsamkeit). Das bedeutet, dass Daten grundsätzlich nach Abschluss der Behandlung zu löschen wären. Die genannten Aufbewahrungspflichten stehen einer Löschung jedoch entgegen, sodass die Pflicht aus Art. 5 DS-GVO erst nach Ablauf der Aufbewahrungsfristen greifen kann.

Unabhängig von der allgemeinen Pflicht der Verantwortlichen zur Datensparsamkeit, haben Betroffene gem. Art. 17 Abs. 1 lit. a) DS-GVO auch das Recht auf Löschung. Sie können von den Verantwortlichen verlangen, dass die sie betreffenden personenbezogenen Daten gelöscht werden, wenn diese zur Aufgabenerfüllung nicht mehr erforderlich sind.

In diesem Bereich erhalte ich regelmäßig Beschwerden, da die Betroffenen bei Ihren Anträgen gegenüber den Verantwortlichen häufig übersehen, dass der Anspruch auf Löschung eingeschränkt wird, wenn Aufbewahrungspflichten dem entgegenstehen (Art. 17 Abs. 3 lit. b) DS-GVO). Das bedeutet: Patienten haben erst nach Ablauf dieser Fristen einen Anspruch auf Löschung ihrer Daten.

3 § 85 Abs. 2 StrlSchG

J.8. Telemedien

8.1 Fanpages – Landesregierung setzt EuGH-Urteil nicht um

Die Entscheidung des Europäischen Gerichtshofs (EuGH) aus dem Jahr 2018 zur gemeinsamen Verantwortlichkeit des Betreibers einer Fanpage und des Unternehmens Facebook war für den Datenschutz sehr wichtig Allerdings führt selbst ein Urteil des EuGH offensichtlich nicht unmittelbar dazu, dass Verantwortliche in der Praxis Konsequenzen ziehen.

Positionierung der DSK: https://t1p.de/Pos-Fanpages

Von der Datenschutzkonferenz (DSK) wurde die Entscheidung des EuGH zu Fanpages bei Facebook durch insgesamt drei Veröffentlichungen bekannt gemacht: eine Entschließung vom 5. Juni 2018, einen Beschluss vom 5. September 2018 sowie eine Positionierung vom 1. April 2019. Fazit aller drei Papiere ist, dass ein datenschutzkonformer Betrieb einer Fanpage vorerst nicht möglich ist.

Addendum von Facebook nicht ausreichend

Facebook hat zwar auf die EuGH-Entscheidung reagiert und ein Addendum als Vertrag über die gemeinsame Verantwortlichkeit veröffentlicht. Ein solcher Vertrag ist eine zwingende Voraussetzung der Datenschutz-Grundverordnung (DS-GVO). Allerdings wurde mittlerweile bereits die zweite geänderte Version des Addendums von einer Arbeitsgruppe der DSK überprüft – mit dem Ergebnis, dass dieses nicht ausreichend ist, um die Vorgaben des Datenschutzrechts zu erfüllen. Darüber hinaus bestehen vor allem bezogen auf Personen, die keinen Account bei Facebook haben, erhebliche Zweifel, auf welche Rechtsgrundlage der Seitenbetreiber die Übermittlung der Nutzerdaten beim Aufruf der Fanpage an Facebook stützen will. Einwilligungen werden für diesen Vorgang nicht eingeholt.

Öffentliche Stellen haben Vorbildfunktion

Aufforderung, Seiten zu deaktivieren

Die Entscheidung des EuGH gilt gleichermaßen für öffentliche wie für nichtöffentliche Stellen, die eine Fanpage bei Facebook betreiben. Allerdings vertrete ich die Auffassung, dass die öffentlichen Stellen in besonderer Weise an die Einhaltung gesetzlicher Vorschriften gebunden sind. Sie haben eine Vertrauensstellung gegenüber der Gesellschaft zu erfüllen und sollten eine Vorbildfunktion ausüben.

Daher informierte ich zunächst mit Schreiben vom 21. Juni 2018 die Staatskanzlei und alle niedersächsischen Ministerien über die Entscheidung des EuGH. Das Schreiben enthielt die klare Aufforderung, bestehende Fanpages (unverzüglich) zu deaktivieren. Auf dieses Schreiben erhielt ich keine Reaktion. Die Überprüfung der Fanpages bei Facebook ergab, dass unter anderem der Ministerpräsident, einige Mitglieder des Kabinetts sowie das Umweltministerium aktiv Fanpages betrieben.

Landesregierung handelt bewusst datenschutzwidrig

Auf ein weiteres Schreiben an die betroffenen Stellen, das ich Ende Mai 2019 versandt habe, erhielt ich schließlich Anfang Juli 2019 eine schriftliche Stellungnahme der Staatskanzlei im Namen der gesamten Landesregierung. Darin wird bestätigt, dass das Unternehmen Facebook hinter den Vorgaben der DS-GVO zurückbleibt und weitere Maßnahmen zur Herstellung der Rechtskonformität notwendig seien.
Es sei dennoch in einer Gesamtabwägung zwischen dem Verstoß gegen die DS-GVO durch den Betrieb von Fanpages durch Teile der Landesregierung einerseits und der „Wahrnehmung des Informationsauftrags und der notwendigen Öffentlichkeitsarbeit in Zeiten der Politikverdrossenheit andererseits“ bewusst entschieden worden, die sozialen Netzwerke Facebook und Instagram weiterhin zu nutzen. Zudem weist die Staatskanzlei darauf hin, dass es auch darum ginge, „den Bürgerinnen und Bürgern in Niedersachsen zu zeigen, dass Politikerinnen und Politiker ganz normale Menschen mit Schwächen und Stärken sind und mitunter auch mal schräge Dinge tun.“ Die Landesregierung handelt somit bewusst und gewollt datenschutzwidrig.

Vormachtstellung von Facebook gefestigt

Der Abwägungsentscheidung der Staatskanzlei kann ich nicht zustimmen. Das Verhalten der Landesregierung bestätigt und festigt die Vormachtstellung des Unternehmens Facebook in seinem datenschutzwidrigen Geschäftsgebaren. Solange sich nicht einmal die staatlichen Stellen aus dem sozialen Netzwerk zurückziehen, wird kein Änderungsdruck auf das Unternehmen ausgeübt. Gerade diese müssen als Vorbild wirken, an dem sich u.a. Wirtschaftsunternehmen orientieren können.

Durchsetzung des EuGH-Urteils wird erschwert

Durch den fortgesetzten Betrieb der Fanpages der Landesregierung fühlen sich die Unternehmen unter Umständen darin bestätigt, ebenfalls nicht auf die Nutzung von Facebook zu verzichten. Letztlich verhält sich die Landesregierung nicht nur datenschutzwidrig, sondern bewirkt zudem, dass mir die Rechtsdurchsetzung der EuGH-Entscheidung auch im nicht-öffentlichen Bereich gegenüber Unternehmen, Handwerk, Freiberuflern und Vereinen erheblich erschwert wird.

Ende Oktober 2019 wurde von Facebook ein überarbeitetes Addendum veröffentlicht, mit dem sich die DSK auseinandersetzt. Mit einer Bewertung und einer Abstimmung des weiteren Vorgehens rechne ich im ersten Quartal 2020.

Mir ist bewusst, dass primär Maßnahmen gegen Facebook selbst getroffen werden müssten. Solange dies nicht geschieht, ist das Vorgehen gegenüber Behörden und Unternehmen nur als

Mittel zweiter Wahl anzusehen. Doch bedauerlicherweise übt die für Facebook zuständige irische Datenschutzaufsichtsbehörde bislang zu wenig Druck aus, um das Unternehmen zu einer tatsächlichen Kurskorrektur zu bewegen. Allerdings kann und darf dies nicht dazu führen, dass ein rechtswidriger Zustand geduldet wird.

Ich werde mich dafür einsetzen, dass in der DSK eine bundeseinheitliche Vorgehensweise für den Umgang mit Fanpages von öffentlichen und nicht-öffentlichen Stellen erreicht werden kann. Darüber hinaus wird die DSK die notwendigen Schritte einleiten, um auf europäischer Ebene die anderen Mitgliedstaaten davon zu überzeugen, dass ein gemeinschaftliches Vorgehen gegen Facebook notwendig ist.

Einheitliches Vorgehen gegen Facebook nötig

Ich sehe es auch 2020 als eine wichtige Aufgabe an, in meinem Zuständigkeitsbereich weiter darauf hinzuwirken, dass die Entscheidung des EuGH in Niedersachsen in der Praxis umgesetzt wird.

8.2 Kampagne "Stop Spying On Us"

Anfang Juni 2019 legte das Netzwerk Datenschutzexpertise bei einigen deutschen Aufsichtsbehörden Beschwerde gegen die massenhafte Datenverarbeitung bei personalisierter Online-Werbung ein. Diese Beschwerde war der Auftakt zur bundesweiten Kampagne „Stop Spying On Us".

Die Unterzeichner der Beschwerde sind die Vorsitzenden der Menschenrechts- und Digitalrechtsorganisationen Digitale Gesellschaft, Netzwerk Datenschutzexpertise, Digitalcourage und des Datenschutzverbandes Deutschland. Konkret rügen sie das vom Interactive Advertising Bureau (IAB)[1] standardisierte OpenRTB-System und „Authorized Buyers" von Google und tragen „erhebliche Datenschutzbedenken beim Einsatz von verhaltensbasierter Internetwerbung" vor.

Informationen zur Kampagne: https://t1p.de/stop-spying

Beide Systeme dienen dem sogenannten Real-Time Bidding und dem Real-Time Advertising. Hierbei handelt es sich um Methoden des Online-Marketings, bei denen Werbeflächen auf Webseiten in Echtzeit an Werbetreibende versteigert werden. Der Versteigerer stellt den potenziellen Bietern Informationen über die aktuellen Nutzer der Webseite zur Verfügung. Der Werbetreibende kann dann einschätzen, ob eine Werbung für ihn ratsam ist oder nicht.

Abgabe an zuständige Behörden

Die eingereichte Beschwerde wurde auch als Musterbeschwerde online abrufbar gemacht. Meine Behörde erhielt insgesamt sechs Beschwerden von Personen, die sich der Kampagne angeschlossen hatten. Sie richten sich zwar gegen Google und gegen alle Unternehmen, die Mitglied des IAB Europe sind. Da allerdings keines dieser Unternehmen einen deutschen Firmensitz in Niedersachsen hat, habe ich keine örtliche Zuständigkeit für die Bearbeitung der Beschwerden. Ich habe diese daher an die jeweils zuständigen Aufsichtsbehörden abgeben.

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

Die Konferenz der deutschen Datenschutzaufsichtsbehörden (DSK) stimmte im Juni 2019 ein einheitliches Vorgehen zu dieser Kampagne ab. Aufgrund der hohen Komplexität des Themas dauert die Beschwerdebearbeitung aber noch an. Ich gehe davon aus, dass DSK die Ergebnisse im Laufe des Jahres 2020 der Öffentlichkeit präsentieren wird.

1 Internationaler Wirtschaftsverband der Online-Werbungsbranche

J.9. Videoüberwachung

9.1 Videoüberwachung in Bus und Bahn

Der Verkehrsbetrieb ÜSTRA wurde von mir – wie bereits im Tätigkeitsbericht 2017/18 dargestellt – per Anordnungsbescheid aufgefordert, die Videoüberwachung in Bussen und Stadtbahnen einzustellen. Im Klageverfahren sahen das Verwaltungsgericht Hannover und in zweiter Instanz das Oberverwaltungsgericht (OVG) Lüneburg die Videoüberwachung als zulässig an. Das OVG ließ eine Revision nicht zu, wogegen ich Nichtzulassungsbeschwerde beim Bundesverwaltungsgericht (BVerwG) eingelegt habe. Diese wurde jedoch zurückgewiesen.

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

Zunächst ist bemerkenswert, dass es sich nach der jüngsten Rechtsprechung des BVerwG bei den Bescheiden meiner Behörde regelmäßig um keine sogenannten Dauer-Verwaltungsakte handelt. Für die Frage der Rechtmäßigkeit der Videoüberwachung muss also allein auf die Rechtslage zum Zeitpunkt der behördlichen Entscheidung abgestellt werden.

Dazu auch Beitrag F.5, S. 56

Das OVG Lüneburg hatte dies noch anders bewertet und war von einem Dauer-Verwaltungsakt ausgegangen, für den die aktuelle (neue) Rechtslage maßgeblich gewesen wäre. Die Entscheidung des BVerwG hat daher zur Folge, dass für meinen Bescheid eine andere Rechtsgrundlage zugrunde zu legen ist als diejenige, welche die Vorinstanz als einschlägig betrachtet hatte.

Leider konnte ich diese höchstrichterliche Rechtsansicht noch nicht bei meiner Entscheidung für die Einlegung der Nichtzulassungsbeschwerde berücksichtigen. Das BVerwG hatte sich in einem anderen Verfahren erst am 27. März 2019 und damit nach Einlegung der Beschwerde entsprechend geäußert.

Begründung der Nichtzulassungsbeschwerde

Auf Grundlage der Entscheidung des OVG hatte ich die Nichtzulassungsbeschwerde im Wesentlichen auf die Nichtanwendbarkeit des zu diesem Zeitpunkt neu in Kraft getretenen § 4 des Bundesdatenschutzgesetzes (BDSG) als Rechtsgrundlage gestützt. Dieser entsprach inhaltlich der Vorgängerregelung, welche das OVG seiner Entscheidung zu Grunde gelegt hatte.

Kein Raum für Anwendung von § 4 BDSG

Denn § 4 BDSG ist nach mehrheitlicher Auffassung der Datenschutzaufsichtsbehörden als nicht europarechtskonform einzustufen, soweit der nicht-

öffentliche Bereich betroffen ist.[1] Art. 6 Abs. 1 lit. f der Datenschutz-Grundverordnung (DS-GVO) enthält eine abschließende Regelung zur Videoüberwachung in öffentlich zugänglichen Räumen durch nicht-öffentliche Stellen. Bestätigt wurde diese Einschätzung von der jüngsten Rechtsprechung des BVerwG, die mangels Öffnungsklausel in der DS-GVO für den nationalen Gesetzgeber für private Stellen keinen Raum für eine Anwendung des § 4 BDSG sieht.

Dementsprechend wäre hier eine Vorlage zur Frage der Vereinbarkeit der angewendeten Vorschrift mit den einschlägigen europarechtlichen Vorgaben an den Europäischen Gerichtshof geboten gewesen. Eine solche Vorlage ist durch das OVG Lüneburg jedoch nicht erfolgt. Dies habe ich in der Begründung meiner Beschwerde gegen die Nichtzulassung der Revision als wesentlichen Aspekt hervorgehoben.

Beschluss des BVerwG

In Anwendung seiner aktuellen Rechtsprechung, wonach für die Bewertung der Rechtmäßigkeit meines Bescheides auf § 6b des BDSG alter Fassung abzustellen ist, wies das BVerwG meine Beschwerde über die Nichtzulassung der Revision zurück. Das BVerwG vertrat die Auffassung, dass ein Interesse an einer datenschutzrechtlichen Beurteilung der Videoüberwachung nach der alten Rechtslage aufgrund der mittlerweile wirksam gewordenen DS-GVO nicht vorläge.

Das BVerwG hat dabei jedoch explizit klargestellt, dass mit der Entscheidung keinerlei Aussage über die Rechtmäßigkeit eines etwaigen Bescheides unter Anwendung der neuen Rechtslage nach der DS-GVO getroffen werde. Hierzu wäre eine weitere eigenständige Prüfung durch die LfD erforderlich.

1 Vergleiche auch Entschließung der 92. DSK vom 09.11.2016: „Videoüberwachungsverbesserungsgesetz zurückziehen!".

9.2 Unzulässige Videoüberwachung im Wald

Immer mehr Jagdpächter setzen Wildkameras ein, um beispielsweise eingerichtete Futterplätze für Wildtiere zu überwachen oder um die Wildbestände zu erfassen. Dabei wird nicht immer daran gedacht, dass auch Menschen erfasst werden können.

Mich erreichte die Beschwerde eines Betroffenen, von dem Aufnahmen einer Wildkamera in einer WhatsApp-Gruppe verbreitet worden waren. Zwei Jagdpächter, die entfernt von ihrem Revier wohnen, hatten eine Person vor Ort beauftragt, die eingesetzten Wildkameras regelmäßig zu sichten und die Aufnahmen an sie weiterzuleiten. Die dort gemachten Aufnahmen wurden teilweise aber auch in einer größeren WhatsApp-Gruppe verbreitet, nämlich dann, wenn man die Personen identifizieren wollte, die sich an den Futterplätzen aufgehalten hatten.

Orientierungshilfe Videoüberwachung mit Wildkameras https://t1p.de/Wildkameras

Zahlreiche Datenschutzverstöße

Grundsätzlich wäre die Überwachung zur Wildzählung auf Grundlage eines berechtigten Interesses (Art. 6 Abs. 1 lit. f DS-GVO) denkbar. Dies hat der Verantwortliche auch erkannt und als Zweck im Verzeichnis der Verarbeitungstätigkeiten angegeben. Dann hätten die Kameras jedoch auch so ausgerichtet werden müssen, dass sich die Erfassungsbereiche auf die Futterplätze beschränkten. Da zur Wildzählung keine detailgenauen Aufnahmen erforderlich sind, wären darüber hinaus die Höhe und auch die Bildschärfe so zu wählen, dass Personen möglichst nicht erkennbar sind.

Auch hätten die Aufnahmen mit Personenbezug umgehend gelöscht werden müssen (Art. 17 Abs. 1 Buchstabe a DS-GVO), anstatt sie weiterzugeben. Weder die Speicherung noch die Weitergabe waren zur Zweckerfüllung erforderlich. Hierfür lag auch keine Erlaubnisnorm vor. Ein besonderes Problem stellt dabei die Nutzung von WhatsApp dar.

Nutzung von WhatsApp problematisch

Daneben wurde hier eine Person vor Ort mit der Erhebung und Verarbeitung in Form der Speicherung, Übermittlung und Löschung beauftragt. Somit hätte ein Auftragsverarbeitungsvertrag im Sinne des Art. 28 DS-GVO abgeschlossen werden müssen.

Kameras wurden demontiert

Im Verlauf des Kontrollverfahrens zeigten sich die Verantwortlichen einsichtig, demontierten die Wildkameras und gaben an zukünftig auf den Einsatz von Wildkameras verzichten zu wollen. Aus diesem Grund wurde von mir auf ein Ordnungswidrigkeitenverfahren verzichtet. Ich weise jedoch darauf hin, dass sich hieraus kein Muster für künftige ähnliche Fälle ableiten lässt.

Unabhängig von diesem Ergebnis dürfen jagdwirtschaftliche Futterplätze grundsätzlich nicht betreten werden (§ 2 Absatz 2 des Niedersächsischen Jagdgesetzes). Sofern mit einer Videoüberwachung unbefugtes Betreten und Beschädigungen nachgewiesen werden sollen, muss das Betretungsverbot in jedem Fall kenntlich gemacht werden.

9.3 Kamera-Attrappe vorgetäuscht

Im Rahmen eines Prüfverfahrens behauptete ein Verantwortlicher, dass es sich bei der von ihm eingesetzten Kamera um eine Attrappe handele. Diese Angabe war allerdings falsch. Ich habe deshalb ein Ordnungswidrigkeitenverfahren eingeleitet.

Meine Behörde erreichte eine Beschwerde wegen der mutmaßlichen Überwachung des öffentlichen Verkehrsraumes durch eine Privatperson. Im anschließenden Prüfverfahren gab der Verantwortliche an, dass es sich bei der vermeintlichen Kamera lediglich um eine Attrappe handele.

Verfahren zunächst beendet

Da mit einer Attrappe zunächst einmal keine personenbezogenen Daten verarbeitet werden können, beendete ich das Verfahren und teilte dem Beschwerdeführer mit, dass keine Überwachung des öffentlichen Verkehrsraumes stattfinde.

Verfahren wieder aufgenommen

Mein Abschlussschreiben konnte der Beschwerdeführer nicht nachvollziehen, da der Verantwortliche in einem gerichtlichen Verfahren sogar Videomaterial vorgelegt habe, welches mit den vermeintlichen Attrappen gefertigt worden sei. Damit lag für mich ein ausreichender Anlass vor, das Verfahren wieder aufzunehmen.

Zahlreiche Verstöße

Im Rahmen der erneuten Ermittlungen machte der Verantwortliche geltend, dass die Überwachung der Straße nur stattfinde, wenn eine Bewegung auf seinem Grundstück erkannt würde. Das erfolge zum Schutz seines Eigentums. Allerdings ist die Erfassung des öffentlichen Verkehrsraumes zum Schutz des Eigentumes mangels Erforderlichkeit im Sinne des Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DS-GVO) grundsätzlich rechtswidrig. Die Bilddaten wurden zudem mit 60 Tagen unverhältnismäßig lange gespeichert. Auch die Hinweisbeschilderung entsprach nicht den Vorgaben des Art. 13 DS-GVO. Besonders problematisch war auch die Nutzung einer Audiofunktion. Die unbefugte Aufzeichnung des vertraulich gesprochen Wortes kann auf Antrag des Betroffenen mit einer Freiheitsstrafe von bis zu drei Jahren oder Geldstrafe bestraft werden (§ 201 Abs. 1 und 2 StGB). Die Kamera ist inzwischen abgebaut. Dennoch sprach ich gegenüber dem Verantwortlichen eine Verwarnung aus.

Lüge führt zu Ordnungswidrigkeitenverfahren

Ein Verantwortlicher muss der Aufsichtsbehörde alle Informationen bereitstellen, die für die Erfüllung ihrer Aufgaben erforderlich sind (Art. 58 Abs. 1 lit. a in Verbindung mit Art. 31 DS-GVO). Da dies in diesem Fall durch die falsche Angabe nicht geschehen ist, habe ich zu diesem Verstoß ein Ordnungswidrigkeitenverfahren eingeleitet, das zum Ende des Berichtszeitraums noch nicht abgeschlossen war.

9.4 Rechtswidrige Videoüberwachung am Arbeitsplatz

Beschäftigte dürfen nicht permanent am Arbeitsplatz überwacht werden. Als ich ein Unternehmen darauf aufmerksam machte, zeigte es sich scheinbar einsichtig. Doch bei einer erneuten Kontrolle stellte ich fest, dass die Kameras immer noch oder wieder in Betrieb waren. Nun droht dem Unternehmen ein Bußgeld.

Im Rahmen eines anlasslosen ersten Kontrollverfahrens wurde die Videoüberwachungsanlage eines Einzelhandelsunternehmens näher überprüft. Bei einer Vor-Ort-Kontrolle stellte sich heraus, dass in den vier Verkaufsstellen des Unternehmens mehrere Kameras die nicht für Kunden zugänglichen Arbeitsplätze der Beschäftigten permanent erfassten. Außerdem fehlte die notwendige Hinweisbeschilderung.

Unternehmen ist zunächst einsichtig

Nach der Ankündigung meiner Behörde, eine Anordnung zur Beseitigung der rechtswidrig betriebenen Videoüberwachung zu erlassen, zeigte sich das Unternehmen zunächst einsichtig. Die Einstellungen der Kameras wurden so verändert, dass diese nur noch Bildaufzeichnungen von den Verkaufsräumen anfertigten. Des Weiteren wurden die Speicherdauer auf 72 Stunden begrenzt und Hinweisschilder angebracht. Daher konnte ich zu diesem Zeitpunkt auf eine Anordnung verzichten.

Dauerüberwachung grundsätzlich unzulässig

Wann eine Videoüberwachung von Arbeitsplätzen datenschutzrechtlich zulässig ist regelt § 26 des Bundesdatenschutzgesetzes (BDSG). Mit der Regelung werden die Interessen von Arbeitgebern und Arbeitnehmern in Bezug auf den Beschäftigtendatenschutz ausgeglichen.

Unzulässige Arbeits- und Leistungskontrolle

Hierbei gelten die vom Bundesarbeitsgericht entwickelten Grundsätze. Danach wird die Grenze einer zulässigen Videoüberwachung überschritten, wenn die Beschäftigten permanent an ihrem Arbeitsplatz überwacht werden und keine strafrechtlichen Handlungen im Raum stehen. Die Videoüberwachung ist dann als eine unzulässige Arbeits- und Leistungskontrolle seitens des Arbeitgebers zu werten.

Kameras gehen wieder in Betrieb

Obgleich das Unternehmen mir gegenüber versicherte, die beanstandeten Mängel beseitigt zu haben, kam es zu einer Beschwerde und damit zu einem zweiten Kontrollverfahren. Erneut wurde eine Vor-Ort-Kontrolle durchgeführt.

Hierbei stellte sich heraus, dass ein Teil der bereits beanstandeten Kameras wieder in Betrieb waren und erneut die Beschäftigten an ihren Arbeitsplätzen lückenlos überwachten.

Ausbleibende Reaktion führt zu Zwangsgeld

Mit einer aufsichtsrechtlichen Maßnahme ordnete ich daher an, die Arbeitsplatzbereiche aus der Videoüberwachung umgehend herauszunehmen. Da das Unternehmen zunächst nicht reagierte, setzte ich wenig später ein Zwangsgeld in Höhe von 2.300 Euro fest und drohte weitere Maßnahmen an. Schließlich lenkte das Unternehmen ein und setzte die beanstandeten Kameras vollständig außer Betrieb. Das Verwaltungsverfahren wurde daher erneut eingestellt.

Bußgeldverfahren eingeleitet

Im Rahmen des ersten Kontrollverfahrens wurde das Unternehmen umfassend über die rechtlichen Grenzen einer Videoüberwachung von Beschäftigten am Arbeitsplatz aufgeklärt. Es ist daher nicht zu tolerieren, dass es trotz dieser Kenntnis erneut zu einer rechtswidrigen, nahezu identisch durchgeführten Überwachung gekommen ist. Wegen dieser offensichtlichen Uneinsichtigkeit des Arbeitgebers habe ich mich entschlossen, ein Ordnungswidrigkeitenverfahren einzuleiten.

Zum Ende des Berichtszeitraums war dieses Verfahren noch nicht abgeschlossen.

9.5 Videoüberwachung am Arbeitsplatz – hohe Anforderungen an Einwilligung

Ein Unternehmen hat seine Produktionshallen und sein Gelände, auf dem auch andere Unternehmen angesiedelt sind dauerhaft mit Kameras überwacht. Es holte dazu zwar Einwilligungen von Betroffenen ein, diese waren aber nicht wirksam. Ich ordnete daraufhin an, die Kameras zumindest am Tag abzustellen, wogegen das Unternehmen gerichtlich vorging.

In einem Prüfverfahren teilte mir ein Unternehmen mit, dass es sein gesamtes Gelände zum Schutz vor Einbrüchen dauerhaft mit Kameras überwacht. Dabei nahm es jedoch nicht nur den Außenbereich der selbst genutzten Gebäude, sondern auch die Gebäude der anderen Unternehmen auf dem Grundstück, die Beschäftigten in den Produktionshallen sowie teilweise die Straße und Nachbarhäuser ins Visier. Da die ganztägige Überwachung bereits aufgrund der fehlenden Erforderlichkeit nicht auf Art. 6 Abs. 1 lit. f Datenschutz-Grundverordnung (DS-GVO) gestützt werden konnte, bat ich das Unternehmen, die Überwachung auf die Nachtstunden zu begrenzen, in denen das Grundstück geschlossen ist.

Betrieb soll nur nachts überwachen

Einwilligung erfüllt nicht die Vorgaben

Daraufhin holte das Unternehmen von den anderen ansässigen Betrieben Einverständniserklärungen zur ganztägigen Videoüberwachung ein. Der Text des verwendeten Vordrucks enthielt jedoch weder die Speicherdauer der Daten noch wurde auf die Möglichkeit des Widerrufs hingewiesen. Da somit die Bedingungen gemäß Art. 7 DS-GVO für eine Einwilligung nicht vorlagen, kam Art. 6 Abs. 1 lit. a DS-GVO als Rechtsgrundlage für die Videoüberwachung nicht in Frage.

Zudem waren auch Kunden, Lieferanten und Beschäftigte (sowohl eigene als auch der Fremdunternehmen) von der Videoüberwachung betroffen. Da von diesen ebenfalls keine wirksamen Einwilligungen vorlagen und aufgrund des damit verbundenen hohen Aufwands in der Regel auch nicht eingeholt werden können, war weiterhin keine Bedingung zur Rechtmäßigkeit gem. Art. 6 Abs. 1 DS-GVO erfüllt. Ich forderte das Unternehmen daher erneut auf, Bereiche außerhalb des Grundstücks von der Kameraerfassung auszunehmen und die Überwachungszeiten auf die Schließzeiten des Grundstücks zu beschränken. Weiter verlangte ich, die Speicherdauer zu begrenzen, die fehlenden Angaben nach Art. 13 DS-GVO (Informationspflichten) auf der Hinweisbeschilderung zu ergänzen und mir das Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO zuzusenden. Im Rahmen einer Anhörung gab ich dem Unternehmen Gelegenheit, dazu Stellung zu nehmen.

Muster für Hinweisschild: https://t1p.de/muster-video

Keine Zeit für die Aufsichtsbehörde

Der Kamerabetreiber teilte mir daraufhin mit, er habe mir in der Angelegenheit schon ausreichend Unterlagen zur Verfügung gestellt und hätte keine Zeit, sich mit mir auseinander zu setzen. Zudem übersandte er mir eine Einverständniserklärung in die Videoüberwachung, die alle seine Beschäftigten unterschrieben hätten. Allerdings waren über den Umfang der Überwachung noch weniger Angaben niedergelegt, als in der zuvor eingeholten Einverständniserklärung der weiteren Unternehmen.

Einwilligung im Beschäftigtenverhältnis meist kritisch

Kurzpapier der DSK „Einwilligungen nach der DS-GVO": https://t1p.de/kp-einwilligung

Da ich das Unternehmen im Vorfeld über die Voraussetzungen einer wirksamen Einwilligung aufgeklärt hatte, wies ich das Unternehmen – wie zuvor angedroht – gemäß Art. 58 Abs. 2 lit. d und f DS-GVO förmlich an, die Verarbeitung personenbezogener Daten mittels Videoüberwachung mit der DS-GVO in Einklang zu bringen. Für die Außerbetriebnahme der Kameras während der Betriebszeiten ordnete ich zudem Sofortvollzug an.

Letzteres ergab sich aus der besonderen Situation der Videoüberwachung im Beschäftigtenverhältnis. Der Verordnungsgeber hat für die Datenverarbeitung im Beschäftigtenkontext mit Art. 88 DS-GVO die nationalen Gesetzgeber ermächtigt, eigene Regelungen zu treffen. Für Deutschland liegt eine solche Regelung mit § 26 Bundesdatenschutzgesetz (BDSG) vor. Nach Absatz 2 der Vorschrift sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen.

Gegen meine Anweisungen hat das Unternehmen Klage eingelegt.

Gericht: Kein Erlaubnistatbestand vorhanden

In seinem Beschluss vom 13. August 2019, Aktenzeichen 10 B 1883/19, hat das Verwaltungsgericht Hannover den Antrag auf Wiederherstellung der aufschiebenden Wirkung als unbegründet abgelehnt. Es führte dazu aus, dass die Videoüberwachung in diesem Fall nicht durch einen gesetzlichen Erlaubnistatbestand des § 26 BDSG gedeckt sei, da sie weder zur Aufdeckung von Straftaten erforderlich sei (§ 26 Abs. 1 Satz 2 BDSG) noch zur Durchführung des Beschäftigtenverhältnisses (§ 26 Abs. 1 Satz 1 BDSG) oder auf Grundlage einer Einwilligung gemäß § 26 Abs. 2 BDSG erfolge.

Zur Einwilligung führte das Gericht unter anderem aus, dass bei der Beurteilung der Freiwilligkeit einer Einwilligung auch der Zeitpunkt der Abgabe maßgeblich sei. So waren zum Zeitpunkt der Einwilligung die Kameras bereits installiert. Somit war die Hürde für die Beschäftigten, abzulehnen und dadurch diese Investition des Arbeitgebers zunichte zu machen, besonders hoch. Weiter sei der Zwang zur Unterschrift durch einen gewissen Gruppenzwang erhöht, da alle Beschäftigten auf demselben Schriftstück unterschreiben sollten. Ein wirtschaftlicher oder rechtlicher Vorteil für die Beschäftigten sei durch die Überwachung nicht erkennbar. Zudem fehle die Information, welche Folgen eine Ablehnung der Überwachung hätte.

Die Kameras in der Produktionshalle wurden aufgrund des Beschlusses während der Betriebszeiten außer Funktion genommen. Das Hauptverfahren war zum Ende des Berichtszeitraums noch nicht abgeschlossen.

J.10. Fotografien

10.1 Veröffentlichung von Fotos durch öffentliche Stellen

Fotos und die Datenschutz-Grundverordnung (DS-GVO) – das ist schon im privaten Bereich nicht immer einfach. Doch wie ist die Rechtslage, wenn staatliche Stellen, zum Beispiel im Rahmen der Öffentlichkeitsarbeit, zur Kamera greifen?

„Wir als Stadtverwaltung möchten ein Sommerfest durchführen. Was müssen wir bei den Fotografien beachten?"

„Wir sind eine Berufskammer und veranstalten einen Nachwuchstag. Müssen wir alle ausladen, die sich nicht vorher mit Fotos einverstanden erklären?"

Anfragen dieser Art erreichen mich regelmäßig. Das Engagement der Anfragenden bei der Organisation solcher Veranstaltungen ist groß – und die Erwartungen der öffentlichen Stellen an die Öffentlichkeitsarbeit sind es ebenfalls. Oft ist das Erstaunen groß, dass auch für Fotografien im Rahmen der Öffentlichkeitsarbeit einer öffentlichen Stelle eine Rechtsgrundlage erforderlich ist.

Ich möchte anhand der Rechtslage darstellen, wie eine öffentliche Stelle unter Beachtung der DS-GVO Fotografien im öffentlichen Bereich anfertigen und veröffentlichen kann.

Rechtsgrundlage erforderlich

Wichtig ist, dass man sich zunächst Folgendes klarmacht: Wenn eine öffentliche Stelle Fotos veröffentlicht, auf denen Personen identifizierbar sind, liegt eine Datenverarbeitung vor. Diese Datenverarbeitung durch die öffentliche Stelle bedarf einer Rechtsgrundlage. Das gilt erst recht dann, wenn zugleich besondere Kategorien personenbezogener Daten[1] betroffen sind. Das ist schon dann der Fall, wenn auf den Fotos Brillen, Rollstühle und andere Gesundheitsdaten erkennbar sind. Dann muss zusätzlich eine Rechtsgrundlage vorliegen, die die Anforderungen des Art. 9 DS-GVO erfüllt.

1 i.S.v. Art. 9 Abs. 1 DS-GVO

Behörde kann nicht berechtigtes Interesse geltend machen

Im Gegensatz zu Privatpersonen und nicht-öffentlichen Stellen kann sich eine öffentliche Stelle nicht auf ein berechtigtes Interesse stützen.[2] Das ergibt sich aus der ausdrücklichen Regelung des Art. 6 Abs. 1 Satz 2 DS-GVO, wonach die Rechtsgrundlage „Buchstabe f" nicht für Behörden in Erfüllung ihrer Aufgaben gilt. § 3 des Niedersächsischen Datenschutzgesetzes (NDSG) zur Zulässigkeit der Verarbeitung findet in diesem Zusammenhang ebenfalls keine Anwendung.

Einwilligung muss freiwillig sein

Kurzpapier der DSK „Einwilligungen nach der DS-GVO": https://t1p.de/kp-einwilligung

Fotos, die im Rahmen behördlicher Öffentlichkeitsarbeit angefertigt werden, können daher nur auf eine Einwilligung der Betroffenen gestützt werden.[3] Die Betroffenen müssen ihre Einwilligung stets freiwillig erteilen. Dieser Grundsatz bekommt hier eine besondere Bedeutung, weil Behörden und andere öffentliche Stellen, die im Rahmen ihrer Aufgaben bzw. begleitend zur Öffentlichkeitsarbeit Fotos veröffentlichen, sich grundsätzlich in einem sogenannten Über-/Unterordnungsverhältnis befinden. Daher müssen die öffentlichen Stellen anhand aller Umstände besonders gründlich prüfen, ob die Einwilligung freiwillig erteilt wurde (Erwägungsgrund Nr. 43 zur DS-GVO). Die Freiwilligkeit ist vor allem dann zu bejahen, wenn die Betroffenen die Einwilligung verweigern können, ohne Nachteile zu erleiden (z. B. ohne von der Veranstaltung ausgeschlossen zu werden, vgl. Erwägungsgrund Nr. 42 und Art. 7 Abs. 4 DS-GVO).

Wenn Fotos im Zusammenhang mit Pflichtveranstaltungen gemacht werden (z. B. in der Schule), kann die Einwilligung mangels einer echten Wahlmöglichkeit nicht freiwillig sein. Auch Gruppendruck sollte vermieden werden. Wenn dies beachtet wird, kommt außerhalb von Pflichtveranstaltungen die Freiwilligkeit einer Einwilligung in Betracht.

Daher ist eine freiwillige Einwilligung beispielsweise möglich bei Festen, Ehrungen, Preisverleihungen und Informationsveranstaltungen von Kommunen bzw. anderen öffentlichen Stellen. Im schulischen Bereich kommen sie z. B. bei der Einschulungsfeier, bei Klassenfotos im Schulgebäude, Fotos auf Klassenfahrten und Ausflügen bzw. in Jahrbüchern in Betracht.

Die eingangs zitierte Anfrage einer Berufskammer ist daher so zu beantworten: Wenn die Teilnahme an der Veranstaltung zwingend mit dem Anfertigen und Veröffentlichen von Fotos verknüpft wird, dann kann von einer nachteilsfreien, d.h. freiwilligen Einwilligung keine Rede sein. Die Berufskammer darf daher nur dann Fotos veröffentlichen, wenn sie die Teilnahme an der Veranstaltung nicht mit einer Einwilligung verknüpft. Mit anderen Worten: Es muss sichergestellt sein, dass die Einwilligung freiwillig erfolgt.

2 Art. 6 Abs. 1 Satz 1 lit. f DS-GVO

3 Die Einwilligung ist in Art. 6 Abs. 1 lit. a DS-GVO und Art. 7 DS-GVO geregelt.

10.2 Veröffentlichung von Personenfotografien durch Vereine

Zahlreiche Vereine treibt die Sorge vor Bußgeldern um, wenn Fotos aus dem Vereinsleben ohne schriftliche Einwilligung aufgenommen und veröffentlicht werden. Um diesen Sorgen entgegenzutreten, stelle ich Fallkonstellationen aus meiner Beratungspraxis vor und erläutere die Rechtslage zu diesem Thema.

Das Kunsturhebergesetz (KUG), das in der Vergangenheit auf die Veröffentlichung von Personenfotografien angewandt wurde, kann nach meiner Ansicht seit der Geltung der Datenschutz-Grundverordnung (DS-GVO) nicht mehr bei jeder Veröffentlichung von Personenfotografien (Bildnissen) herangezogen werden. Ein Rückgriff auf das KUG ist nur noch zu journalistischen, künstlerischen, wissenschaftlichen oder literarischen Zwecken möglich, wobei die Öffentlichkeitsarbeit (z. B. eines Vereins) keine Verarbeitung zu journalistischen Zwecken darstellt. In allen übrigen Fällen bedarf es für die Veröffentlichung von Personenfotografien einer Rechtsgrundlage nach der DS-GVO. Dennoch ändert sich für diejenigen, die Personenfotografien zu anderen als den genannten Zwecken verarbeiten möchten, gar nicht so viel.

So viel ändert sich gar nicht

Das KUG hatte (und hat) den Grundsatz, dass für die Veröffentlichung von Personenfotografien eine Einwilligung der abgebildeten Person(en) erforderlich ist. Auf eine Einwilligung konnte in der Vergangenheit nur in den im KUG geregelten Ausnahmefällen (z. B. Bildnisse aus dem Bereich der Zeitgeschichte oder Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen) verzichtet werden.[1]

Seit Geltung der DS-GVO muss jede Verarbeitung von personenbezogenen Daten, die nicht unter den Anwendungsbereich des KUG fällt, auf eine Rechtsgrundlage aus Art. 6 Abs. 1 DS-GVO gestützt werden. Hier kommen u.a. in Betracht:

- eine Einwilligungserklärung (Art. 6 Abs. 1 lit. a DS-GVO),
- ein Vertrag (Art. 6 Abs. 1 lit. b DSG-VO) oder
- eine Interessenabwägung (Art. 6 Abs. 1 lit. f DS-GVO).

Mögliche Rechtsgrundlagen

Wenn ein Verein bislang für die Veröffentlichung von Personenfotografien Einwilligungserklärungen eingeholt hat, dann kann er diese Praxis fortführen. Hat er sich hingegen bei seinen Veröffentlichungen auf einen der Ausnahmefälle des KUG gestützt und auf eine Einwilligungserklärung verzichten können, dann kommt nun die Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f. DS-GVO in Betracht.

1 Selbst wenn einer dieser Ausnahmefälle zunächst bejaht werden konnte, sah (und sieht) auch das KUG eine Interessenabwägung und einen Ausschluss der Befugnis zur Veröffentlichung vor, wenn dadurch ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben war, seiner Angehörigen verletzt würde – die Ausnahme von der Ausnahme.

Wichtiges zur Interessenabwägung

Im Rahmen der Interessenabwägung sind folgende Aspekte zu berücksichtigen:

Das müssen Vereine bei der Abwägung beachten

- Bei welcher Gelegenheit werden die Fotos angefertigt? Handelt es sich um eine öffentliche Veranstaltung, wie z. B. ein Vereinsfest oder einen Wettkampf oder um ein nichtöffentliches Training?
- Über welche Kanäle soll veröffentlicht werden? Soll das Foto in einer Printausgabe der Vereinszeitung, auf der Vereinshomepage und/oder in sozialen Netzwerken veröffentlicht werden?
- Sind auf den Bildern nur Erwachsene oder auch Kinder und Jugendliche unter 16 Jahren zu erkennen?
- Hat die konkrete, für die Veröffentlichung geplante Aufnahme einen kompromittierenden, sexistischen oder sonstigen verletzenden Inhalt?

Vereinszeitung als Printversion

Grundsätzlich gilt, dass die Veröffentlichung von Fotos, die während einer öffentlichen Veranstaltung angefertigt wurden, auf denen nur Erwachsene zu erkennen sind und die ausschließlich über Printmedien verbreitet werden, in der Regel auf eine Interessenabwägung gestützt werden kann. Im Rahmen der Interessenabwägung kann ein berechtigtes öffentliches Interesse an der Berichterstattung über die Veranstaltung sowie ein berechtigtes Interesse des Vereins an Eigenwerbung berücksichtigt werden. Überwiegende Interessen von Betroffenen, also fotografierten Personen, die einer Veröffentlichung entgegenstehen könnten, werden in den meisten Fällen nicht vorliegen.

Fotos von Kindern in der Vereinszeitung

Besonders umsichtig abwägen

Bei der geplanten Veröffentlichung von Kinderfotos auf Basis einer Interessenabwägung ist besondere Umsicht gefragt. Es ist zwar nicht grundsätzlich ausgeschlossen, dass die Verarbeitung von personenbezogenen Daten von Kindern auf eine Interessenabwägung gestützt werden kann. Allerdings mit der Einschränkung, dass in der Regel von einem überwiegenden und der Verarbeitung entgegenstehenden Interesse des Kindes auszugehen ist.

Es müssen somit im konkreten Einzelfall besondere Aspekte angeführt werden können, die ausnahmsweise für eine Veröffentlichung der Aufnahmen von Kindern sprechen. So ein Aspekt könnte zum Beispiel die Erwähnung besonderer sportlicher Erfolge eines minderjährigen Sportlers in der Berichterstattung sein, die um ein Foto ergänzt wird.

Veröffentlichung im Internet

Bei einer geplanten Veröffentlichung im Internet sieht die Interessenabwägung hingegen anders aus. Das Internet bietet vielfältige Recherchemöglichkeiten, es ermöglicht eine weltweite Verbreitung und es vergisst nicht. Aus diesem Grund lässt sich eine Verbreitung von Personenfotografien über das Internet, wie z. B. auf der Homepage eines Vereins, grundsätzlich nicht mehr auf eine

Interessenabwägung stützen – ganz gleich ob Erwachsene oder Kinder abgebildet sind. Etwas anderes könnte nur gelten, wenn die Fotos ausschließlich in einem zugangsbeschränkten Bereich für Vereinsmitglieder abzurufen und auch über Suchmaschinen nicht auffindbar wären. Bei einer geplanten Veröffentlichung im Internet müssen Vereine daher in der Regel auf Einwilligungen zurückgreifen.

Veröffentlichung im Internet nur mit Einwilligung

Veröffentlichung in sozialen Medien

Eine Interessenabwägung als Rechtsgrundlage für die Veröffentlichung von Bildern über soziale Medien ist bei Aufnahmen von Erwachsenen und von Kindern ebenfalls nicht denkbar. Hier stehen die Nutzungsbedingungen der Anbieter der sozialen Medien den Interessen der Betroffenen entgegen, so dass vor einer Veröffentlichung in sozialen Medien ebenfalls eine Einwilligung der Abgebildeten (bzw. der Erziehungsberechtigten, sofern es sich bei den Abgebildeten um Kinder handelt) einzuholen wäre.

Auswahl der Bilder und Informationspflichten

Allgemein für alle Veröffentlichungswege gilt, dass keine Bilder mit

- kompromittierendem
- sexistischem oder
- beleidigenden

Inhalt auf Basis einer Interessenabwägung publiziert werden können.

FAQ zu den Informationspflichten: https://t1p.de/infopflichten

Darüber hinaus muss der Verantwortliche unabhängig von einer Rechtsgrundlage für die Veröffentlichung bereits vor der Erstellung der Fotografien eine Information gemäß Art. 13 DS-GVO erteilen. Bei Veranstaltungen wie Vereinsfesten oder Wettkämpfen kann dies z. B. durch Aushänge für Besucher an allen Eingängen zum Festgelände oder zur Sportstätte geschehen. Im Rahmen der Information der Teilnehmer und Besucher ist insbesondere auch auf geplante Veröffentlichungen unter Nennung der konkreten Medienarten einzugehen.

10.3 Reiseveranstalter will Veröffentlichung von Fotos per AGB erzwingen

Ein Veranstalter von Jugend- und Schulreisen veröffentlichte zu Werbezwecken Foto- und Videomaterial von Jugendlichen unter 16 Jahren auf seiner Webseite und in sozialen Medien. In den Allgemeinen Geschäftsbedingungen (AGB) werden die Veröffentlichungen als zu akzeptierende „Voraussetzung für die Buchung und Teilnahme an einer Reise" festgesetzt. Eine Einwilligungserklärung war nicht vorgesehen. Ein klarer Verstoß gegen datenschutzrechtliche Anforderungen.

Über eine Beschwerde wurde ich auf die Geschäftspraxis des Reiseveranstalters aufmerksam. Bei der datenschutzrechtlichen Kontrolle stellte ich fest, dass die Veröffentlichung der Fotos und des Videomaterials auf der eigenen Unternehmenswebseite und erst recht über die Social-Media-Plattformen rechtswidrig ist. Der Reiseveranstalter konnte keine Rechtsgrundlage für diese Verarbeitung nachweisen und wurde von mir verwarnt sowie zur Unterlassung aufgefordert.

Keine wirksame Einwilligung

Der Reiseveranstalter hatte keine wirksamen Einwilligungen der Reisenden eingeholt. Auch fehlten bereits die Voraussetzungen einer wirksamen Einwilligung, die freiwillig, informiert, transparent und eindeutig erteilt werden muss. Die Eindeutigkeit kann sich aus einer Erklärung, aber auch aus einem sonstigen Verhalten ergeben. Das Verhalten muss jedoch eindeutig auf das Einverständnis mit einer Datenverarbeitung zu einem bestimmten Zweck schließen lassen. Im ersten Fall liegt dann eine ausdrückliche, im zweiten Fall eine konkludente Einwilligung vor.

Einwilligung weder ausdrücklich noch konkludent

Eine ausdrückliche Einwilligung wurde von den Reisenden nicht eingeholt. Der Buchungsprozess war nicht so gestaltet, dass die Reisenden neben der Buchung eine von ihr erkennbar getrennte Einwilligung abgeben konnten. Die Reisenden haben auch keine konkludente Einwilligung, etwa durch Buchung der Reise abgegeben. Reisende erklären mit Abschluss eines Reisevertrags ihr Einverständnis damit, dass gegen Bezahlung reisetypische Leistungen erbracht werden. Dies sind der Transport, die Unterbringung und gerade im Falle von Jugend- oder Schulreisen die Betreuung der Jugendlichen. Auf ein Einverständnis mit der Veröffentlichung des Foto- und Videomaterials kann nicht geschlossen werden.

Fotos nicht zur Vertragserfüllung notwendig

Die Veröffentlichung des Foto- und Videomaterials war zur Erfüllung des Vertrages nicht erforderlich, so dass die Voraussetzungen von Art. 6 Abs. 1 lit. b

Datenschutz-Grundverordnung (DS-GVO) nicht vorliegen. Was erforderlich ist oder nicht, richtet sich nicht nach den AGB, die in einen Vertrag einbezogen werden, sondern danach, was die Vertragsparteien als typischen Vertragsinhalt ansehen. Das, was nicht typisch ist, ist auch nicht gemäß Art. 6 Abs. 1 lit. b DS-GVO datenschutzrechtlich erlaubt. Die Veröffentlichung von Foto- und Videomaterial ist keine typische Leistung eines Reisevertrags. Sie dient ausschließlich der Werbung für den Reiseveranstalter. Zwar können auch Datenverarbeitungen gesetzlich erlaubt sein, die zur Durchführung vorvertraglicher Maßnahmen notwendig sind. Hierunter fallen jedoch nur solche Datenverarbeitungen, die auf Anfrage der Betroffenen erfolgen.

Fotos dienen nur zur Werbung

Kein überwiegendes berechtigtes Interesse

Gesetzlich erlaubt sind gemäß Art. 6 Abs. 1 lit. f DS-GVO auch Datenverarbeitungen, die zur Wahrung eines berechtigten Interesses erforderlich sind. Und zwar dann, wenn das Interesse des Verarbeiters an der Durchführung gegenüber dem Interesse des Betroffenen am Unterlassen der Verarbeitung überwiegt. Diese Voraussetzung war nicht erfüllt. Kinder und Jugendliche unter 16 Jahren sind – wie die Vorschrift betont – besonders schutzbedürftig. Damit fallen die Risiken, die mit einer Veröffentlichung von Abbildungen im Internet einhergehen (unbefugte Vervielfältigung, Manipulation, Missbrauch, globale Verfügbarkeit), erschwerend ins Gewicht.

Keine Erlaubnis nach KUG

Eine Erlaubnis zur Veröffentlichung des Foto- und Videomaterials ergab sich auch nicht aus dem Kunsturhebergesetz (KUG). Danach sind Veröffentlichungen von Fotos und Videos von Menschen auch ohne deren Einwilligung zulässig, wenn ein zeitgeschichtliches Ereignis oder eine Versammlung vorliegen, die Abgebildeten in den Hintergrund treten oder die Veröffentlichung künstlerischen Zwecken dient.

Ein solcher Fall lag nicht vor. In den Veröffentlichungen standen die Jugendlichen im Vordergrund und es fehlte der Bezug zu zeitgeschichtlichen Ereignissen und Versammlungen. Die Veröffentlichungen dienten gewerblichen und damit nicht künstlerischen Zwecken. Letztlich waren diese Aspekte aber zweitrangig, denn der erhöhte Schutzbedarf von Jugendlichen wirkt sich spätestens im Rahmen der durchzuführenden Interessenabwägung nach § 23 Abs. 2 KUG zulasten der Veröffentlichung aus.

Verpixelung reicht aus

Der Reisveranstalter konnte meiner Unterlassungsanordnung dadurch genügen, indem er die abgebildeten Jugendlichen verpixelte und das Videomaterial kürzte. Eine vollständige Entfernung der Fotos und Videos war nicht notwendig.

Im Dialog mit dem Unternehmen konnten wichtige Eckpunkte für eine datenschutzkonforme Einwilligungserklärung skizziert werden. Damit ist dieser Fall ein Beispiel dafür, dass Kontrolle und Beratung sich nicht ausschließen, sondern ergänzen können.

Beratung und Kontrolle

10.4 Einwilligung zur Veröffentlichung von Personenfotografien

Als Rechtsgrundlage für die Veröffentlichung von Personenfotografien wird, sofern überwiegende Veröffentlichungsinteressen gem. Art. 6 Abs. 1 lit. f der Datenschutz-Grundverordnung (DS-GVO) oder eine spezialgesetzliche Ermächtigungsgrundlage, wie § 23 des Kunsturhebergesetzes (KUG) nicht in Betracht kommen,[1] häufig auf eine Einwilligungserklärung zurückgegriffen. Diese Einwilligung muss die Anforderungen der DS-GVO erfüllen. Das gilt für öffentliche Stellen ebenso wie für Unternehmen oder Vereine, die Bilder mit Personenbezug veröffentlichen möchten. Da dieses Thema immer wieder zu Fragen führt, gebe ich hier einen Überblick, worauf beim Inhalt einer Einwilligungserklärung zu achten ist.

Zwar schreibt die DS-GVO keine Schriftform für Einwilligungserklärungen vor, zu empfehlen ist sie aber dennoch. Denn auf diesem Weg lässt sich eine Anforderung aus Artikel 7 Abs. 1 DS-GVO leicht erfüllen: die Nachweispflicht des Verantwortlichen über die Einwilligung des Betroffenen, in diesem Fall der fotografierten Person.[2]

Eine schriftliche Einwilligung ist in verständlicher und leicht zugänglicher Form abzufragen sowie in einer klaren und einfachen Sprache zu formulieren.

Freiwilligkeit und Widerruf

Die Einwilligung muss grundsätzlich freiwillig gegeben werden und darf mit keinerlei Zwang verbunden sein. So darf eine Einwilligung nicht mit einer Leistung des Verantwortlichen verknüpft werden. Beispielsweise dürfen Sportvereine Personen nicht von einer Mitgliedschaft ausschließen, wenn diese nicht bereit sind, eine Einwilligungserklärung zur Veröffentlichung von Fotografien zu unterschreiben. Auch Unternehmen dürfen die Einwilligung nicht für einen Vertragsabschluss voraussetzen oder sie pauschal mit den allgemeinen Geschäftsbedingungen verknüpfen (Lesen Sie hierzu auch unseren Beitrag auf Seite 182. in Kapitel J 10.3). Da Behörden und sonstige öffentliche Stellen Fotografien im Rahmen der Öffentlichkeitsarbeit häufig in einem sogenannten Über-/Unterordnungsverhältnis anfertigen (wie z. B. gegenüber Beschäftigten einer Kindertagesstätte) und veröffentlichen, müssen sie genau prüfen, ob die Einwilligung freiwillig erteilt wird. Das ist vor allem dann zu bejahen, wenn die Betroffenen die Einwilligung verweigern können, ohne Nachteile zu erleiden (z. B. ohne von einer Veranstaltung ausgeschlossen zu werden).

1 s. hierzu auch den Beitrag „Veröffentlichung von Personenfotografien durch Vereine“ auf S. 179

2 bzw. bei Minderjährigen die Einwilligung (auch) der Erziehungsberechtigten, s.u.

Die betroffene Person hat das Recht, die Einwilligung jederzeit ohne Angabe von Gründen zu widerrufen. Hierüber muss der Verantwortliche die einwilligende Person informieren. Der Widerruf muss so einfach erteilt werden können wie die Einwilligung selbst.

Inhalt der Einwilligungserklärung

In jeder Einwilligungserklärung sind die Zwecke der Verarbeitung klar und eindeutig zu benennen. Eine Einwilligung muss ausreichend konkret sein, d.h. darf nicht pauschal für eine Vielzahl von Sachverhalten (z. B. allgemein für die Öffentlichkeitsarbeit) erfolgen. Stattdessen sollten z. B. Veranstaltungen oder Anlässe, in deren Rahmen Personenfotografien aufgenommen werden könnten, bereits in der Einwilligungserklärung aufgeführt werden. Bei verschiedenen Zwecken muss eine selektive Einwilligung – z. B. durch Ankreuzen – möglich sein. Bei der Veröffentlichung von Personenfotografien müssen vor diesem Hintergrund zwingend auch die Wege der Veröffentlichung transparent sein. So genügt es beispielsweise nicht, pauschal davon zu sprechen, dass die Personenfotografien veröffentlicht werden. Stattdessen muss klar benannt werden, auf welchen Kanälen der Verantwortliche eine Veröffentlichung der Fotografien beabsichtigt.

Kurzpapier der DSK „Einwilligun-gen nach der DS-GVO": https://t1p.de/kp-einwilligung

Zugleich muss es der betroffenen Person möglich sein, der Veröffentlichung auf einem Medium (beispielsweise der Webseite des Verantwortlichen) zuzustimmen, während z. B. die Einwilligung zur Veröffentlichung in einem sozialen Netzwerk nicht erteilt wird. Alle geplanten Veröffentlichungskanäle müssen sich aus der Einwilligungserklärung eindeutig ergeben, der Ausschluss einzelner Kanäle muss möglich sein.

Ein Häkchen pro Medium

Dabei ist die Zustimmung zu den einzelnen Verbreitungswegen über Opt-in einzuholen, also beispielsweise durch das Setzen von Kreuzen oder Häkchen. Wege der Veröffentlichung, die in der Einwilligungserklärung nicht aufgeführt sind, weil sie z. B. zum Zeitpunkt der Einwilligung noch gar nicht in Planung und damit für den Betroffenen nicht ersichtlich waren, dürfen für eine spätere Veröffentlichung nicht genutzt werden. In diesem Fall wäre für diesen neuen Veröffentlichungsweg eine weitere Einwilligungserklärung einzuholen.

Besondere Anforderungen für Kinder und Jugendliche

Da sich Kinder und Jugendliche der Risiken und Folgen sowie ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind als Erwachsene, sind besondere Anforderungen zu beachten, wenn von Minderjährigen Einwilligungen eingeholt werden. Sollen diese z. B. für Veröffentlichungen von Personenfotografien durch Sportvereine eingeholt werden, so ist zu prüfen, inwieweit bei den Minderjährigen das erforderliche Maß an Urteils- und Einsichtsfähigkeit vorhanden ist.

Eine starre Altersgrenze für die Einwilligung eines Kindes regelt die DS-GVO nur für die Dienste der Informationsgesellschaft im Internet (16 Jahre). In allen anderen Fällen bedarf es jeweils einer konkreten Einzelfallprüfung. Um den Unsicherheiten bei der Beurteilung der Urteils- und Einsichtsfähigkeit von Minderjährigen zu begegnen, empfiehlt es sich, jedenfalls bei Kindern bis zur Vollendung des 16. Lebensjahres im Zweifel immer die Einwilligung der Erziehungsberechtigten einzuholen. Bei Minderjährigen ab 14 Jahren sollte zusätzlich die Einwilligung der oder des Minderjährigen eingeholt werden.

J.11. Vereine

11.1 Begehrte Mitgliederliste von Hannover 96

Vor der Neuwahl des Aufsichtsrats von Hannover 96 e.V. verlangte eine Gruppe von Mitgliedern vom Verein eine aktuelle Mitgliederliste. Mit den Adress- und E-Mail-Daten sollte eine außerordentliche Mitgliederversammlung einberufen werden. Der Verein lehnte dies jedoch mit Verweis auf den Datenschutz ab.

Der Justitiar von Hannover 96 teilte mir mit, dass der Verein durch das Amtsgericht Hannover dazu verurteilt worden sei, drei Mitgliedern einer Interessengemeinschaft, eine aktuelle und vollständige Liste seiner Mitglieder zu übergeben. Soweit möglich, solle die Liste mit mehr als 20.000 Datensätzen mit einem elektronischen Datenträger (z. B. ein USB-Stick) übermittelt werden. Dem Verein lägen bereits hundert Widersprüche von Mitgliedern gegen die Übermittlung vor.

Viele Mitglieder legen Beschwerde ein

Zeitgleich gingen bei mir etliche Beschwerden von Mitgliedern gegen die Herausgabe ihrer personenbezogenen Daten ein.

Wann ist es zulässig, eine Mitgliederliste zu übermitteln?

Mitglieder sollen über verschiedene Positionen informiert werden

Vereinsmitglieder können ein berechtigtes Interesse daran haben, eine Mitgliederliste zu erhalten. Ein berechtigtes Interesse des einzelnen Mitglieds ist in solchen Fällen anerkannt, in denen beabsichtigt ist, ein – wie hier – nach der Satzung vorgeschriebenes Stimmenquorum zu erreichen, um von den Minderheitenrechten Gebrauch zu machen. Darüber hinaus ist ein berechtigtes Interesse auch dann anzunehmen, soweit es erforderlich ist, um das Recht auf Mitwirkung an der vereinsrechtlichen Willensbildung wirkungsvoll ausüben zu können. Etwa, um andere Mitglieder des Vereins über bestimmte Belange zu informieren oder mit ihnen zu einer Erörterung in Kontakt zu treten.

Im Zuge der bevorstehenden Aufsichtsratswahlen bei Hannover 96 e.V. beabsichtigten die Kläger, die Mitgliederdaten dazu zu verwenden, um in vergleichbarer Weise wie der Verein ihre Auffassung den übrigen Vereinsmitgliedern kund zu tun. Zu diesem Zweck ist ein berechtigtes Interesse an der Überlassung der Mitgliederdaten gegeben. Allerdings muss geprüft werden, ob diesem berechtigten Interesse der Kläger kein überwiegendes Interesse des Vereins oder anderer Vereinsmitglieder gegenübersteht.[1]

1 Art. 6 Abs. 1 Satz 1 lit. f. DS-GVO

Daten vor unberechtigtem Zugriff schützen

Die Mitglieder eines Vereins haben ein berechtigtes Interesse daran, dass ihre Rechte, z. B. auf Information, Auskunft, Löschung und Datenübertragbarkeit, gewahrt werden und die Daten vor unberechtigtem Zugriff durch angemessene technisch- und organisatorische Maßnahmen geschützt werden. Darüber hinaus besteht ein berechtigtes Interesse daran, dass die Daten nicht mehr als zwingend erforderlich dupliziert und an Dritte übermittelt werden.

Im vorliegenden Fall würden die Daten an die Interessensgemeinschaft übermittelt, wodurch der Datenbestand immerhin verdoppelt würde. Die Interessengemeinschaft musste daher gewährleisten, den Betroffenenrechten nachzukommen und angemessene technisch- organisatorische Maßnahmen zum Schutz der personenbezogenen Daten zu ergreifen.

Lösungsansatz im Konfliktfall

Möglicher Kompromiss: Treuhänder

Den berechtigten Interessen der Interessengemeinschaft kann ebenso durch Übermittlung der Daten an einen Treuhänder nachgekommen werden. So käme es auch nicht zu einer ausufernden Duplizierung der Daten. Diese würden vielmehr beim Treuhänder gespeichert und könnten von diesem für die Ausübung der Minderheitenrechte genutzt werden. Bei der Wahl des Treuhänders ist darauf zu achten, dass dieser die Anforderungen der DS-GVO erfüllen kann. Es bestünde so auch die Möglichkeit, sich von den entsprechenden technischen und organisatorischen Maßnahmen beim Treuhänder im Vorfeld sowie bei regelmäßigen Kontrollen zu überzeugen.

Darüber hinaus könnte der Treuhänder überprüfen, ob die Mitteilungen, die das jeweilige Mitglied den anderen Mitgliedern zukommen lassen möchte, rechtlich zulässig sind. Die Nutzung der Mitgliederliste für kommerzielle Werbung oder eine Mitteilung, die einen Verstoß gegen Strafvorschriften beinhalten würde, wäre nämlich illegitim. Ein Treuhänder würde die jeweiligen zulässigen Mitteilungen der Vereinsmitglieder (hier der Interessengemeinschaft) dann entsprechend der erhaltenen Mitgliederliste weiterleiten, wobei er bestehende Widersprüche einzelner Mitglieder zu beachten hat. Die Wahl des Treuhänders sollte auf eine möglichst neutrale Person fallen. Diese Rechtsauffassung deckt sich mit einem Beschluss des Bundesgerichtshofs (BGH) vom 21.06.2010.[2]

So ging es bei 96 weiter

Im konkreten Fall wurde die Beschwerde des Vereins gerichtlich abgewiesen, so dass die Mitgliederliste der Interessengemeinschaft auf einem USB-Stick übergeben wurde.

2 Hierin bestätigt der BGH das zugrunde liegende Urteil des Oberlandesgerichts Hamburg. Danach bleiben die schützenswerten Belange betroffener Vereinsmitglieder gewahrt, wenn die Mitgliederliste an einen Treuhänder herausgegeben wird und somit die andere Seite (also jene Vereinsmitglieder, welche die Liste satzungsgemäß begehren) selbst keinen Einblick in die Liste erhalten und zudem der Treuhänder einen etwaigen Widerspruch einzelner Mitglieder gegen die Weiterleitung der verfassten Schreiben zu beachten hat.

Anwalt bestätigt Vernichtung des USB-Sticks

Der Vorgang war mittlerweile aber durch Presseberichte und eine vereinseigene Information an die Mitglieder öffentlich geworden. Aufgrund der dadurch ausgelösten Kontroverse nahm die Interessengemeinschaft Abstand von ihrem Vorhaben und teilte mit, dass der USB-Stick vernichtet worden sei. Zwischenzeitlich hatte ich Vertreter der Interessengemeinschaft, auch aufgrund der mir vorliegenden Beschwerden, angeschrieben und um Stellungnahme ersucht. Der Rechtsanwalt der Gemeinschaft bestätigte mir die physikalische Vernichtung des USB-Sticks schriftlich. Eine Verarbeitung der personenbezogenen Daten war nicht erfolgt. Das Verfahren wurde beendet.

Fazit

Die Bekanntgabe von Mitgliederdaten zur Ausübung satzungsmäßiger Rechte ist im Vereinsinteresse erforderlich, ohne dass Interessen oder Grundrechte und -freiheiten der betroffenen Person überwiegen.[3] Um Missbräuchen entgegenzuwirken, sollten aber Mitglieder, denen die Adressen bekannt gegeben werden, zusichern, dass die Daten nicht für andere Zwecke verwendet werden.

Bei großen Vereinen oder bei solchen, deren Mitglieder ein Interesse an der vertraulichen Behandlung ihrer Daten haben, oder bei denen die Zugehörigkeit zum Verein als besonders sensibel gilt (z. B. Parteien, Gewerkschaften, Selbsthilfegruppen), können jedoch Interessen oder Grundrechte und -freiheiten der Betroffenen überwiegen. In solchen Fällen bietet sich die Einschaltung eines neutralen Treuhänders an.

Der Treuhänder darf die in der Liste enthaltenen Daten nicht an einzelne Mitglieder weitergeben. Um den übrigen Mitgliedern Gelegenheit zu geben, der Verwendung ihrer Daten durch einen Treuhänder zu widersprechen, sollten alle Mitglieder zudem über das beabsichtigte Vorgehen und ihre Widerspruchsmöglichkeit rechtzeitig vorab über die Vereinsmedien informiert werden. Der Treuhänder muss die ihm von einzelnen Mitgliedern aufgegebenen Untersagungen und Einschränkungen beachten.

3 Art. 6 Abs. 1 lit. f DS-GVO

J.12. Technik

12.1 Weiterentwicklung des Standard-Datenschutzmodells

Mit dem Standard-Datenschutzmodell (SDM) können aus den rechtlichen Vorgaben der Datenschutz-Grundverordnung (DS-GVO) technisch-organisatorische Maßnahmen für die Verarbeitung personenbezogener Daten hergeleitet werden. Das SDM wird gemeinschaftlich von den deutschen Datenschutzaufsichtsbehörden fortentwickelt. Mit dem SDM 2.0a liegt nun eine grundlegend überarbeitete Fassung vor.

Die DS-GVO fordert von Verantwortlichen, über technisch-organisatorische Maßnahmen sicherzustellen, dass Risiken für personenbezogene Daten bereits vor der Verarbeitung geprüft, abgewogen und durch entsprechende Vorkehrungen minimiert werden. Mit der am 6. November 2019 durch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vorgelegten Fassung des SDM wurde die Methode, deren Grundzüge noch unter der Geltung des alten Datenschutzrechts entwickelt worden waren, an Vorgaben und Terminologie der DS-GVO vollständig angepasst.

SDM-Version 2.0a:
https://t1p.de/SDM2a

Das SDM basiert auf folgenden aus der DS-GVO abgeleiteten Gewährleistungszielen:

- Datenminimierung,
- Verfügbarkeit wovon und für wen,
- Integrität von was,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz und
- Intervenierbarkeit.

Rechtssicherheit
für Verantwortliche

Damit unterstützt das SDM Verantwortliche in Wirtschaft und Verwaltung, die von der DS-GVO auferlegten technischen und organisatorischen Maßnahmen sowie die Nachweis- und Rechenschaftspflichten zu erfüllen. Die DSK empfiehlt die neue SDM-Version bei Planung, Einführung und Betrieb von personenbezogenen Datenverarbeitungen anzuwenden.

Die bereits als erforderlich erkannten technischen oder organisatorischen Sicherungsmaßnahmen lassen sich einem standardisierten Maßnahmenkatalog entnehmen, der als Anhang zum SDM konzipiert ist. Der Maßnahmenkatalog befindet sich noch in der Erarbeitungsphase. Die einzelnen Bausteine des Katalogs werden sukzessive veröffentlicht und zur Anwendung freigegeben. Vorgesehen ist dies für das Jahr 2020.

12.2 ZAWAS – Prozess zur Auswahl angemessener Sicherungsmaßnahmen in der Praxis

Im Jahr 2018 hat meine Behörde die Erprobungsfassung einer Methodik zur Auswahl angemessener technischer-organisatorischer Sicherungsmaßnahmen (ZAWAS) als systematische, praxisbezogene Handlungsempfehlung für Verantwortliche bereitgestellt. Sie sollten damit bei der datenschutzkonformen Gestaltung von Verarbeitungstätigkeiten unterstützt werden. Im Berichtszeitraum wurde der Prozess nun vielfach in Prüfungen und Beratungen angewendet.

ZAWAS beschreibt einen Prozess in acht Schritten, an dessen Ende die Auswahl angemessener technisch-organisatorischer Maßnahmen steht. Eine zentrale Forderung der Datenschutz-Grundverordnung (DS-GVO) ist, dass Verantwortliche das zu erwartende Risiko einer Datenverarbeitung bewerten müssen. Deshalb besteht ein großer Teil von ZAWAS aus einer umfangreichen Risikoanalyse, für die der Prozess auf das niedersächsische Schutzstufenkonzept zurückgreift. Die Methode sieht außerdem vor, dass die ergriffenen Maßnahmen regelmäßig evaluiert werden.

Informationen zu ZAWAS: https://t1p.de/ZAWAS

Prozess nun auch in Beratungen empfohlen

In Schulungen meines hauseignen Datenschutzinstituts gebe ich Datenschutzbeauftragen eine Einführung in die Grundlagen des technisch-organisatorischen Datenschutzes. In diesem Rahmen wird auch ZAWAS behandelt. Aufgrund zahlreicher positiver Rückmeldungen von Kursteilnehmerinnen und -teilnehmern empfehle ich den ursprünglich für Schulungszwecke konzipierten Prozess inzwischen auch bei Beratungen.

Ebenso finden die Prüfungen meines Hauses im Bereich des technisch-organisatorischen Datenschutzes und deren Auswertung nach dieser Methode statt. Als „Proof of Concept" habe ich den Prozess im Rahmen meiner Querschnittsprüfung von 50 Unternehmen der niedersächsischen Wirtschaft (mehr zu dieser Prüfung ab Seite 142) erstmals umfassend angewendet. Er war Ausgangspunkt für die Auswertung der Antworten auf die Frage zur Datenschutz-Folgenabschätzung. Dabei ging es darum, ob die in Art. 35 Abs. 7 DS-GVO vorgeschriebenen Inhalte vorhanden waren.

Anwendung im Rahmen der Querschnittsprüfung

Da ZAWAS sich im Rahmen dieser Prüfung bewährt hat, ist es nun die Grundlage für künftige Prüfungen zur systematischen Herangehensweise im technisch-organisatorischen Datenschutz. Von den geprüften Unternehmen habe ich zahlreiche Rückmeldungen mit dem Hinweis erhalten, dass der Prozess zukünftig Basis für ihre unternehmensinternen Leitfäden zur datenschutzkonformen Gestaltung von Verarbeitungstätigkeiten sein wird.

Interesse an ZAWAS nimmt zu

Keine Pflicht zur Anwendung

Es besteht zwar keine Pflicht den Prozess ZAWAS zu nutzen, aber ich empfehle dies allen Verantwortlichen. Bei sachgemäßer Anwendung bietet ZAWAS dem Verantwortlichen die Sicherheit, dass bei der Gestaltung der Verarbeitungstätigkeiten alle datenschutzrelevanten Faktoren betrachtet werden und nachvollziehbaren Ergebnisse entstehen. Das gilt insbesondere für Verarbeitungstätigkeiten, die eine Datenschutz-Folgenabschätzung erfordern.

Auch jenseits der niedersächsischen Landesgrenzen steigt das Interesse an ZAWAS. Dies wird an einer zunehmenden Zahl von Vortragsanfragen zu diesem Thema deutlich.

Nachdem das Standard-Datenschutzmodell (SDM) konkretisiert und Ende 2019 grundlegend überarbeitet wurde (siehe Beitrag SDM, S. 189), wird meine Behörde die SDM-Praxishilfe, als die ZAWAS konzipiert wurde, im Jahr 2020 weiter erproben. Über den bisherigen Anwendungsbereich hinaus untersucht meine Behörde, in welchem Umfang sich ZAWAS auf die Informationssicherheit übertragen lässt. Ich gehe beispielsweise davon aus, dass sich Synergien erzielen lassen, sofern in einigen Teilschritten oder sogar ganzen Schritten des Prozesses die datenschutzrechtliche Prüfung und Sicherstellung der Informationssicherheit gebündelt werden können.

12.3 DSK veröffentlicht Prüfschema für Windows 10

Auf meine Initiative hin hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden ein Prüfschema für Windows 10 veröffentlicht. Hiermit können Verantwortliche kontrollieren und nachweisen, ob Windows 10 im jeweiligen Nutzerumfeld datenschutzkonform eingesetzt wird.

Microsofts Betriebssystem Windows 10 wird seit seiner Einführung insbesondere wegen der Übermittlung von Telemetriedaten kritisch betrachtet. Dies gilt vor allem für Systemzustands- und Diagnosedaten, die permanent im Hintergrund an den Hersteller übertragen werden und dabei auch personenbeziehbare Daten enthalten können. Mich hat eine Vielzahl von Anfragen sowohl von öffentlichen Stellen als auch von Unternehmen zum datenschutzkonformen Einsatz von Windows 10 erreicht. Verunsicherte Nutzer und verantwortliche Stellen fragen häufig an, ob der Einsatz von Windows 10 datenschutzrechtlich grundsätzlich unbedenklich ist.

Leider ist es unmöglich, hierzu eine pauschale Aussage zu treffen. Windows 10 wird regelmäßig mit Updates versorgt, die Funktionen verändern. Zudem ist das Produkt in unterschiedlichen Editionen erhältlich und kann durch die jeweiligen Administratoren oder Nutzer konfiguriert und in unterschiedlichen Umgebungen eingesetzt werden. Im Fokus des Datenschutzrechts steht die Frage, was der Inhalt der übermittelten Telemetriedaten ist und ob die Übermittlung nach der DS-GVO rechtmäßig ist.

Prüfschema Windows 10: https://t1p.de/Pruefschema-Windows10

Ein Arbeitskreis der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat sich daher unter meiner Leitung mit der Frage beschäftigt, wie Windows 10 datenschutzrechtlich bewertet werden kann. Als erstes Ergebnis hat die DSK ein Prüfschema veröffentlicht, anhand dessen Verantwortliche beurteilen können, ob ein bereits laufender oder geplanter Einsatz von Windows 10 datenschutzkonform ist oder wäre.

DSK und Microsoft erarbeiten datenschutzkonforme Konfiguration

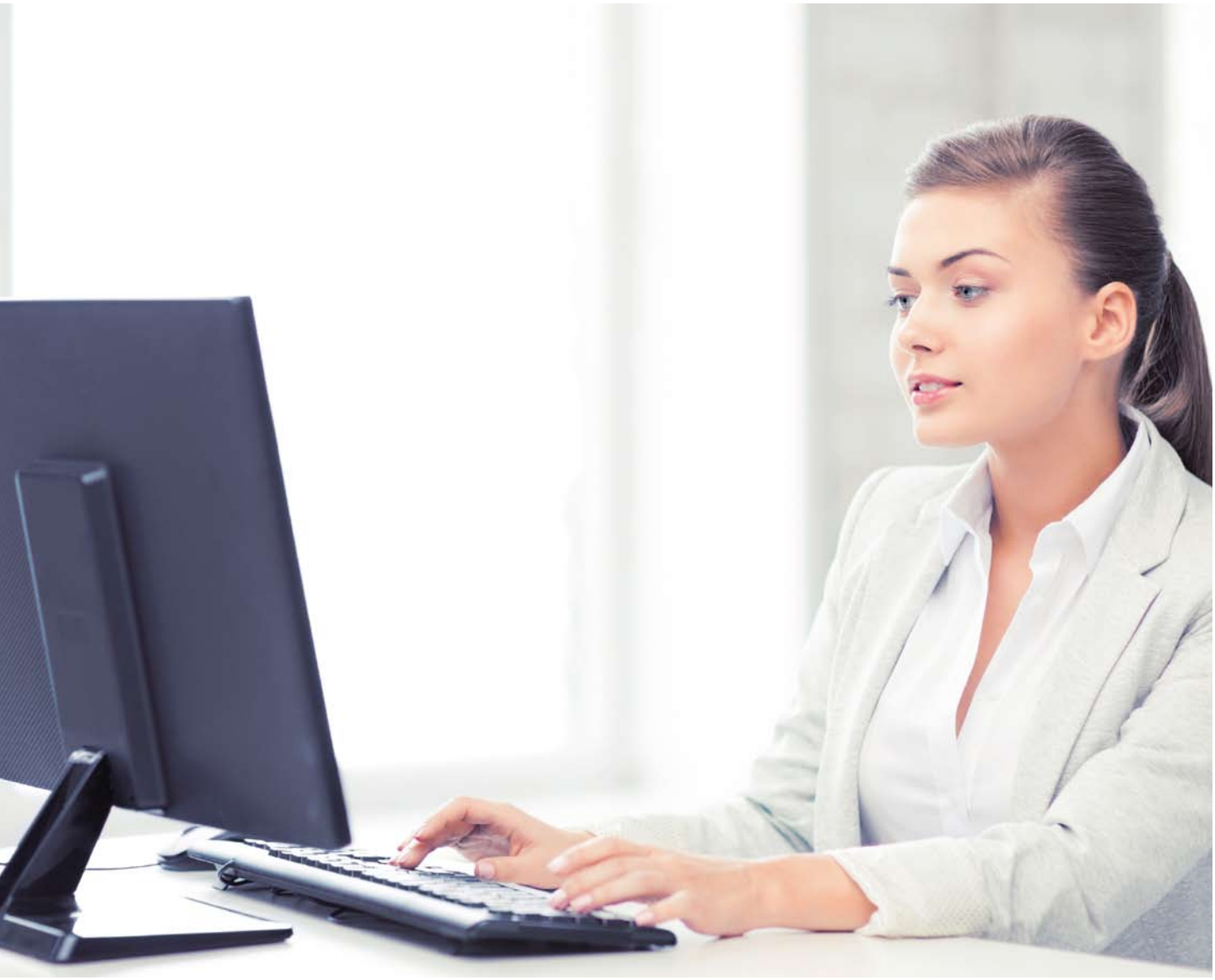
Zunächst muss festgestellt werden, welche Daten an Microsoft übermittelt werden und ob diese einen Personenbezug im Sinne von Art. 4 Nr. 1 DS-GVO aufweisen. Ist das der Fall, muss der Verantwortliche prüfen, ob für die Übermittlung der Daten eine Rechtsgrundlage vorliegt. Fehlt die Grundlage, muss der Verantwortliche prüfen, ob ihm Maßnahmen zur Verfügung stehen, mit denen er die Übermittlung personenbezogener Telemetriedaten verhindern kann.

In einem ersten Schritt habe ich dazu die für große Unternehmen und öffentliche Verwaltungen relevante Version „Windows 10 Enterprise“ analysiert. Gemeinsam mit Microsoft wurde eine Konfiguration gefunden, bei der eine datenschutzkonforme Übertragung von Telemetriedaten erreicht worden ist (mehr dazu in Kapitel 12.6., S. 199).

Home und Pro noch ohne passende Konfiguration

Für die Versionen Windows 10 Home und Windows 10 Pro, die häufig bei kleinen und mittelgroßen Unternehmen sowie Kommunen eingesetzt werden, hat Microsoft entsprechende Möglichkeiten zur Konfiguration leider noch nicht zur Verfügung gestellt.

Meine Arbeit an diesem Thema ist daher noch nicht beendet. Ich werde im Jahr 2020 prüfen, ob der Einsatz von Windows 10 in der niedersächsischen Landesverwaltung entsprechend dieser Vorgaben erfolgt. Zudem befindet sich die DSK weiter in Gesprächen mit Microsoft. Sofern sich hieraus konkretere Vorgaben für den Einsatz von Windows 10 ergeben, werde ich diese den Verantwortlichen mitteilen.



12.4 Emotet: Angriffe auf Vertraulichkeit und Integrität

Im Jahr 2019 wurden meiner Behörde 46 Datenschutzverletzungen gemeldet, die auf einen Angriff durch Emotet zurückzuführen waren. In 16 Fällen waren öffentliche Stellen betroffen; bei 30 Angriffen waren private Stellen wie z. B. Unternehmen Opfer einer Emotet-Attacke. Auch 2020 wird der Virus mit hoher Wahrscheinlichkeit eine erhebliche Bedrohung darstellen.

Der Trojaner Emotet bedroht vorrangig gespeicherte Daten, die während eines Angriffs verschlüsselt werden und somit für den Nutzer nicht mehr verfügbar sind. Im Anschluss nutzt das Programm zur weiteren Verbreitung das Adressbuch des Mailclients sowie auf dem System verfügbare Nachrichten, um auf dieser Basis neue Nachrichten zu versenden. Dabei nimmt Emotet bewusst Bezug auf die vorherige Kommunikation des Angegriffenen, um beim Empfänger besonders authentisch und echt zu wirken. So ist auch die Vertraulichkeit der echten Kontakte und Nachrichteninhalte bedroht.

Besonders größere Unternehmen betroffen

Aktueller Virenschutz hilft nur bedingt

Die versendeten Nachrichten enthalten meist Office-Dokumente, die beim Öffnen das Nachladen weiterer Schadprogrammkomponenten aus dem Internet initiieren. Da die einzelnen Komponenten regelmäßig überarbeitet werden, ist ein aktueller Virenschutz nur bedingt in der Lage, derartige Angriffe zu erkennen und abzuwehren.

Von Emotet sind besondere größere Unternehmen und Einrichtungen betroffen, da diese vermeintlich in der Lage sind, erhebliche Lösegelder für ihre verschlüsselten Daten zu zahlen. In Niedersachsen sind vor allem die Fälle der Medizinischen Hochschule Hannover und der Stadt Neustadt am Rübenberge aus dem September 2019 sowie des Heise-Verlages vom Juni 2019 öffentlich geworden[1].

Als weiteres Angriffsszenario verschafft Emotet dem Angreifer direkten Zugriff auf die Netze des Opfers, z. B. über das Remote Desktop Protokoll (RDP), das eigentlich Wartungszugängen dient. Spätestens in diesem Stadium ist das gesamte Netzwerk des Opfers kompromittiert.

1 vergl. Medienberichte https://www.heise.de/newsticker/meldung/Emotet-befaellt-Medizinische-Hochschule-Hannover-4541189.html, https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Neustadt-erholt-sich-nur-langsam-von-Trojaner,neustadt334.html, https://www.heise.de/ct/artikel/Trojaner-Befall-Emotet-bei-Heise-4437807.html

Vorbeugende Maßnahmen

Zur Abwehr von Emotet-Angriffen empfehle ich folgende Maßnahmen:

Das können Sie tun

- Einsatz von Software zur Erkennung von Schadprogrammen,
- regelmäßige Updates der eingesetzten Betriebssystem- und Anwendungskomponenten,
- weitere Einzelmaßnahmen, die in Kommunikation zwischen angegriffenem Rechner und dem Angreifer-Server eingreifen, welche für einen Angriff nötig ist:

Makros deaktivieren

  - Deaktivieren von Makros: MS-Office- (vorrangig Word) Dokumente werden dazu genutzt, über integrierte Makros die nächste Stufe der Schadprogramme nachzuladen. Daher sollten Makros von der Systemadministration per Gruppenrichtlinie deaktiviert werden. Sofern man auf Makros in eingehenden Dokumenten nicht angewiesen ist, könnten diese auch durch ein Filterprogramm auf dem Mailserver entfernt, oder die Dokumente dort ins PDF-Format konvertiert werden. Alternativ kann man Open-Office oder Libre-Office verwenden, um Nachrichtenanhänge zu öffnen, da diese Programme keine MS-Office-Makros unterstützen.
  - Isolieren der Internetverbindung: Vielfach einfacher und gegen ein weiteres Spektrum von Schadprogrammen wirksam ist es, für den Benutzer bzw. das Benutzerkonto, das Zugriff auf Nachrichteneingänge hat, den Internetzugriff mittels http-Protokoll zu sperren. Hierzu bietet sich eine Browser-Virtualisierung an. Ein altes (seit 2006) und nach wie vor bewährtes Konzept ist das ReCoBS des BSI[2]. Von Nachteil ist der hohe Aufwand sowie die hierfür erforderliche Netzbandbreite (insbesondere für multimediale Internetinhalte). Dafür bietet dieser Ansatz maximalen Schutz.

Virtualisierung des Browsers

Alternativ kann der Browser auf dem Arbeitsplatzrechner mit einem rudimentären Betriebssystem in einer Virtualisierungsumgebung genutzt werden. Bekannteste Lösung am Markt ist hier die im Auftrag des BSI entwickelte Browser-In-The-Box-Lösung Bitbox. Dieser Ansatz basiert auf der in der freien Version quelloffenen Virtualisierungslösung Virtualbox[3] und kann daher prinzipiell auch einfach von IT-Abteilungen oder IT-Dienstleistern nachgebaut und implementiert werden. Auch eine Nutzung fertiger virtueller Maschinen mit Browser ist möglich. Einen ähnlichen Ansatz der Anwendungsisolierung in einer Sandbox verfolgt das kommerzielle Produkt Bromium[4], das auf Mikrovirtualisierung setzt.

2 Weitere Informationen über die ReCoBS-Lösung beim Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/recobslanginfo_pdf.pdf

3 GNU-Lizenzierte Virtual Box bei Oracle: https://www.virtualbox.org/ und Open-Source Betriebssysteme z. B. bei OSBoxes.org: https://www.osboxes.org/virtualbox-images/, sowie https://tails.boum.org/doc/advanced_topics/virtualization/virtualbox/index.de.html

4 vergl. https://www.bromium.com/our-tech/bromium-secure-platform/

Browser-Virtualisierung ist ein seit mehr als einem Jahrzehnt etablierter Ansatz zur Absicherung der Internetnutzung. Je nach Variante ist diese Lösung mit geringem Aufwand und Kosten realisierbar und bietet einen hohen Schutz nicht nur gegen die Ausbreitung von Emotet, sondern gegen eine ganze Reihe weiterer möglicher Angriffe, insbesondere auch im Zusammenhang der Internetnutzung. So empfiehlt das BSI den Einsatz von Virtualisierung des Browsers für Datenverarbeitungen mit hohem Schutzbedarf in der Bundesverwaltung.[5] Angesichts der langen Verfügbarkeit dieses Ansatzes und andererseits der Verpflichtung zur Berücksichtigung des Standes der Technik gemäß Art. 25 DS-GVO ist die Browser-Virtualisierung bereits den niedriger angesiedelten „anerkannten Regeln der Technik" zuzuordnen. Daher sollte der Ansatz ohnehin berücksichtigt werden.

Die einfachste Lösung, die jedoch auch das geringste Sicherheitsniveau bietet, ist es, die Internetnutzung in einen anderen Nutzerkontext auszulagern, der nur Zugriff auf das Internet sowie ein Transferverzeichnis im System vorhält.

Maßnahmen im Fall eines Angriffes:

Ist ein Angriff bereits erfolgt, sollten schnell Maßnahmen ergriffen werden, um die Auswirkungen so gering wie möglich zu halten. Hierzu gehört:

- Das gesamte Netz vom Internet trennen.
- Kommunikationspartner über einen möglichen Befall informieren, damit diese eintreffende Nachrichten mit entsprechender Vorsicht behandeln,
- Infizierte Geräte identifizieren. Hierzu sollte ein aktueller Virenscanner mit eigenem Betriebssystem von einem externen Datenträger gestartet werden. Auf keinen Fall darf auf verdächtigen Systemen eine Anmeldung mit Systemverwalterkonten erfolgen. Sonst besteht die Gefahr, dass sich das Schadprogramm die zusätzlichen Berechtigungen zunutze macht, um auf direktem Wege weitere Systeme (insbesondere Server) im Netz zu infiltrieren.
- Befallene Systeme sind komplett (einschließlich des Betriebssystems) neu aufzusetzen, da nicht auszuschließen ist, dass auch Systemdateien manipuliert wurden. Außerdem sollten sämtliche Kennworte zurückgesetzt werden, da die Angriffe auch darauf zielen, Zugangsdaten abzugreifen.

Systeme komplett neu aufsetzen

Einen Überblick zu den Maßnahmen mit denen sich ein Emotet-Befall bekämpfen lässt, bieten die Veröffentlichungen des Heise-Verlages über dessen eigenen Befall[6].

5 Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG für den sicheren Einsatz von Web-Browsern in der Bundesverwaltung, Seite 6: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Sichere_Web-Browser.pdf

6 Berichterstattung bei Heise Online mit einem Beitrag zur Best Practice:
- https://www.heise.de/select/ct/2019/13/1561119412274300
- https://www.heise.de/newsticker/meldung/heiseshow-Emotet-trifft-Heise-Einblicke-in-einen-Trojaner-Angriff-4439850.html
- https://www.heise.de/security/meldung/Emotet-bei-Heise-Schaeden-von-weit-ueber-50-000-Euro-4444155.html

12.5 Orientierungshilfe zur Verschlüsselung von E-Mails

Sowohl in der Verwaltung als auch in der Wirtschaft treibt Verantwortliche die Frage um, wie sich die Vorgaben der Datenschutz-Grundverordnung bei der E-Mail-Verschlüsselung erfüllen lassen. Der Arbeitskreis Technik der Datenschutzkonferenz (DSK) hat aufgrund der Vielzahl von Anfragen zu diesem Thema mit der Arbeit an einer Orientierungshilfe zur E-Mail-Verschlüsselung begonnen.

Stand der Technik als Basis für Anforderungen

Die Orientierungshilfe soll unter anderem aufzeigen, welche Anforderungen an die Verfahren zum Versand und zur Entgegennahme von E-Mails durch Verantwortliche, ihre Auftragsverarbeiter und öffentliche E-Mail-Diensteanbieter zu erfüllen sind. Der Stand der Technik zum Veröffentlichungszeitpunkt soll als Ausgangspunkt für die Konkretisierung der Anforderungen dienen. Damit richtet sich die Orientierungshilfe an den Anforderungen nach Art. 24, 25 und 32 Datenschutz-Grundverordnung (DS-GVO) aus.

Verantwortliche und Auftragsverarbeiter[1] sind gesetzlich verpflichtet, die Risiken, die sich aus ihren Verarbeitungen personenbezogener Daten ergeben, zu minimieren und ein angemessenes Schutzniveau zu gewährleisten. Dazu müssen sowohl den Stand der Technik als auch die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung (im Sinne des Art. 4 lit. 2 DS-GVO), die Implementierungskosten sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden.

Verantwortliche müssen Einzelfall berücksichtigen

Die Orientierungshilfe der DSK wird mit praxisnahen Beispielen arbeiten. Die Verantwortlichen und Auftragsverarbeiter bleiben jedoch verpflichtet, Besonderheiten ihrer Verarbeitungen in jedem Einzelfall zu berücksichtigen.

Risiken wegen Verletzung von Vertraulichkeit und Integrität

Die Orientierungshilfe wird ausschließlich die Risiken, die mit einer Verletzung von Vertraulichkeit und Integrität personenbezogener Daten verbunden sind, behandeln. Sie setzt voraus, dass die Verantwortlichen beziehungsweise ihre Auftragsverarbeiter einschätzen, welche Schäden aus einem Bruch von Vertraulichkeit und Integrität resultieren können.
Die Arbeiten an der Orientierungshilfe dauerten bei Redaktionsschluss dieses Berichts noch an. Die Veröffentlichung ist für 2020 vorgesehen.

1 Auftragsverarbeiter ausschließlich im Hinblick auf ihre Pflichten nach Art. 32 DS-GVO.

12.6 IT-Labor – Prüfungen von Telemedien und Windows 10

Speziell im Bereich von Telemedien und Softwareprodukten lässt sich ein Sachverhalt allein auf Basis in Papierform vorliegender Informationen häufig nicht angemessen beurteilen. Erst durch eine Prüfung im IT-Labor wird die juristische Prüfung um wichtige technische Aspekte erweitert.

Durch die Analyse des IT-Labors wird nachvollziehbar, welche Cookies und Trackingmechanismen von einer Webseite oder einer App genutzt werden. Zudem lässt sich nachverfolgen, welche Server an welchen Standorten in die Datenverarbeitung einbezogen werden, und welche personenbezogenen Daten dabei übertragen werden.

Dabei werden verschiedene Tools eingesetzt, die u. a. in der Lage sind, auch eine verschlüsselte Kommunikation, z. B. mittels https, zwischen Client und Server durch eine „Man in the middle"-Konfiguration, zu analysieren. Hierzu wird der eigentlich vorgesehene direkte Kommunikationskanal zwischen dem Server eines Anbieters (z. B. einer Website) und dem Endgerät eines Benutzers unterbrochen und ein Analysecomputer wird in den unterbrochenen Kommunikationskanal eingefügt. Der Analysecomputer kann dann unter Nutzung eigener Zertifikate die Kommunikation entschlüsseln und den unverschlüsselten Datenverkehr lesen und analysieren.

Tests zur Enterprise-Version von Windows 10

Unter meiner Leitung wurde gemeinsam mit weiteren Landesdatenschutzbehörden ein Prüfschema zur datenschutzkonformen Nutzung von Windows 10 erarbeitet und verabschiedet (Details zum Prüfschema auf Seite 193). Dabei wurde insbesondere die Übermittlung von Telemetriedaten vom Rechner des Nutzers (Client) an Microsoft betrachtet. Im IT-Labor meiner Behörde wurden auf Basis der Windows 10 Enterprise-Version verschiedene Konfigurationen getestet und deren Auswirkungen analysiert.

In einem behördenübergreifenden Workshop, zu dem auch Vertreter von Microsoft eingeladen waren, konnte mit Tools, die von Microsoft zur allgemeinen Nutzung zur Verfügung gestellt wurden, gezeigt werden, dass die Übermittlung von personenbezogenen Telemetriedaten unterbunden werden kann.

Verstärkter Einsatz des IT-Labors vor Ort

Das IT-Labor wird in Zukunft neben der Unterstützung der Beschwerdebearbeitung und eigener Prüfaktivitäten zusätzlich verstärkt im Rahmen von Vor-Ort-Prüfungen zum Einsatz kommen. Prüfungsschwerpunkte werden dabei u.a. die Analyse von Datenbeständen, z. B. in Datenbanken sowie die Beurteilung von Konfigurationseinstellungen und des Betriebs von unternehmenseigenen Apps sein.