daten
schutz


Die
Landesbeauftragte
für den Datenschutz
Niedersachsen

# 24. Tätigkeitsbericht 2017–2018

Niedersachsen

# 24. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2017 – 2018

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

Verantwortlich: Barbara Thiel

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

Bilder, Grafiken: Seite 9, 14, 15, 17, 170: LfD Niedersachsen,
alle weiteren: Ingimage

Druck: Druckhaus Pinkvoss GmbH
Landwehrstraße 85, 30519 Hannover

**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 beider Geschlechter.**

# Inhaltsverzeichnis

# A. Vorwort

**Gemeinhin ist man gut beraten, in Berichten wie dem hier vorliegenden zurückhaltend mit Superlativen umzugehen. Denn nicht selten wird die vermeintliche Rekordmarke schon in einem der folgenden Jahre übertroffen. Trotzdem kann ich ohne Übertreibung feststellen, dass meine Behörde vermutlich nie mehr mit so vielen Neuerungen konfrontiert sein wird wie in den vergangenen beiden Jahren.**

Ein beträchtlicher Teil dieser Veränderungen im Zeitraum des 24. Tätigkeitsberichts wurde von einem für den europäischen Datenschutz historischen Ereignis verursacht: dem Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018. Nach zwei Jahren Übergangsfrist war die Verordnung nun geltendes Recht in allen Mitgliedstaaten der EU. Dass eine solch umfassende Gesetzesreform Fragen, Unsicherheiten und Beratungsbedarf mit sich bringen würde, war absehbar. Nicht umsonst hatten meine Mitarbeiterinnen und Mitarbeiter und ich bereits 2017 in zahlreichen Veranstaltungen auf die neuen Vorschriften hingewiesen und Handreichungen zur DS-GVO-Umstellung für die verantwortlichen Stellen veröffentlicht. Auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder richtete während meines Vorsitzjahres ihr Augenmerk darauf, die kommenden Anforderungen und Erwartungen gegenüber Politik und Wirtschaft zu artikulieren.

Zu meinem Bedauern fanden diese Bemühungen zunächst aber wenig Gehör. Vielen Verarbeitern personenbezogener Daten wurde offenbar erst kurz vor Geltungsbeginn der DS-GVO bewusst, welche Neuerungen nun auf sie zukamen. Dementsprechend groß war die Wucht, mit der die Anfragewelle meine Behörde im Frühjahr 2018 traf. Mehr als 8000 Beratungen führten meine Mitarbeiterinnen und Mitarbeiter, denen ich an dieser Stelle meinen ausdrücklichen Dank ausspreche, allein 2018 durch, um Unternehmen, Vereine, Verbände und öffentliche Stellen zu unterstützen. Dieser Arbeitsschwerpunkt war der allgemein spürbaren Unsicherheit während der Umstellung auf die DS-GVO geschuldet. In Zukunft werde ich mich aber auch wieder stärker der Aufgabe als Aufsichtsbehörde zuwenden und vermehrt Kontrollen und anlasslose Prüfungen durchführen.

*Barbara Thiel*

Doch es gab in den Jahren 2017 und 2018 noch weit mehr zu tun, als sich auf die europäische Datenschutzreform vorzubereiten: Neben zahlreichen Verfahren nach „altem" Recht war meine Behörde in vielen Fällen auch bei der Erarbeitung neuer Gesetze gefragt. Leider musste ich dabei feststellen, dass der Datenschutz – nicht immer, aber häufig – eher als Hindernis und lästige Pflicht betrachtet wird denn als Voraussetzung für die Freiheit des Individuums. Deshalb werde ich auch in den kommenden Jahren weiter konstruktiv dafür streiten, dass den Belangen des Datenschutzes die Bedeutung zugemessen wird, die ihnen gebührt.

Mein nächster Tätigkeitsbericht wird sich nicht mehr mit einem Zeitraum von zwei Jahren befassen, sondern nur noch mit einem. Denn ab sofort werde ich jährlich Bericht erstatten, wie es die DS-GVO verlangt.

# B. Management Summary

## Management Summary – Das Wichtigste in Kürze

Führt man heute in einer beliebigen Runde ein Gespräch zum Thema Datenschutz, schwebt meist die Datenschutz-Grundverordnung (DS-GVO) über allem. Tatsächlich haben die Vorbereitungen auf die Verordnung in den vergangenen beiden Jahren viel Raum eingenommen, sowohl auf europäischer, nationaler und Landesebene als auch in meiner Behörde selbst. Auch habe ich bereits erste anlasslose Prüfungen nach DS-GVO auf den Weg gebracht.

Dabei sollen aber nicht die weiteren, teils noch nach „altem" Recht behandelten Themen unter den Tisch fallen, wie etwa der Datenschutz bei der Polizei, im Gesundheitsbereich oder in der Automobilindustrie.

### Start der DS-GVO und erste Prüfungen

Vorbereitungen der Aufsicht auf die DS-GVO

In Kraft getreten war die Datenschutz-Grundverordnung bekanntlich schon im Mai 2016. Doch mit gutem Grund gewährte der Gesetzgeber eine Übergangszeit von zwei Jahren bis zu ihrer Geltung. Die umfassende Reform verlangte nicht nur von den datenverarbeitenden Stellen einige Vorbereitungen, sondern auch von den Aufsichtsbehörden in der EU. Es galt, Hilfestellungen für die Datenverarbeiter zu erarbeiten, interne Verfahren zur Durchführung der neuen Kooperationsverfahren zu installieren und schließlich den Europäischen Datenschutzausschuss aufzubauen.

Ebenfalls gefragt war der nationale Gesetzgeber, der die Regelungsaufträge und Öffnungsklauseln der DS-GVO in deutsches Recht umsetzen musste.

Neue Gesetze zum Datenschutz auf Bundes- und Landesebene

Das 2017 verabschiedete neue Bundesdatenschutzgesetz enthält nun u.a. eigene Regelungen für die Datenverarbeitung durch öffentliche Stellen, zur Bestellung von betrieblichen Datenschutzbeauftragten, zur Datenverarbeitung im Beschäftigungsverhältnis und zur Vertretung der deutschen Aufsichtsbehörden auf europäischer Ebene sowie zur Zusammenarbeit der deutschen Aufsichtsbehörden untereinander. Auch der Regelungsauftrag bezüglich der Errichtung und der Aufgaben der nationalen Aufsichtsbehörden wurde hier

umgesetzt. Bei den neuen Regelungen zur Videoüberwachung hat der nationale Gesetzgeber seine Spielräume hingegen überstrapaziert.

Grundlegend überarbeitet werden musste zudem das niedersächsische Datenschutzgesetz. Zu meinem Bedauern fand die parlamentarische Beratung dazu unter hohem Zeitdruck statt. Wichtige Forderungen aus meinem Haus blieben letztlich unberücksichtigt.

Prüfungen in Unternehmen und Kommunen

Weitreichende Neuerungen brachte die DS-GVO auch im täglichen Betrieb meiner Behörde mit sich. Dazu zählten nicht nur die massive Zunahme von Beratungsanfragen und gemeldeten Datenpannen, sondern vor allem auch qualitative Aspekte unserer Arbeit. So stellt die DS-GVO etwa ganz neue Anforderungen an die Bearbeitung von Datenschutz-Beschwerden.

Um mir frühzeitig einen Überblick zu verschaffen, ob und wie gut verantwortliche Stellen die Vorgaben der DS-GVO umgesetzt haben, habe ich erste Prüfungen begonnen. Dies betraf einerseits 50 große und mittelgroße Unternehmen mit Hauptsitz in Niedersachsen, die Fragen zu zehn Bereichen des Datenschutzes beantworten sollten. Andererseits war es mir auch wichtig, den öffentlichen Bereich ebenfalls in meine Prüfungen einzubeziehen. Deshalb habe ich Ende 2018 Fragebögen an 150 Gemeinden, Städte und Landkreise verschickt.

Weitere Prüfungen (allerdings nicht ausschließlich nach DS-GVO) führten meine Mitarbeiter beispielsweise in Meldebehörden, bei Abfallentsorgern, in Krankenhäusern und in Schulen durch.

## Telemedien und Technik

Praxishilfe für technisch-organisatorischen Datenschutz

Zweifellos haben sich mit der Einführung der DS-GVO viele praktische Umsetzungsfragen ergeben. Eine Frage mit sehr großer Breitenwirkung ist, welche Datenschutzvorschriften für Betreiber von Webseiten maßgeblich sind. Schließlich gibt es unzählige Webseiten von Unternehmen, öffentlichen Stel-

len, Verbänden, Vereinen und Privatpersonen. Die deutschen Datenschutzbehörden haben sich hierzu in einer Positionsbestimmung deutlich geäußert.

Hohe Anforderungen stellt die DS-GVO unter anderem an den technisch-organisatorischen Datenschutz. Meine Behörde hat deshalb als Praxishilfe den „Prozess zur Auswahl angemessener Sicherungsmaßnahmen" (ZAWAS) entwickelt. Dieser soll verantwortlichen Stellen die Auswahl geeigneter Maßnahmen erleichtern.

## Der EuGH setzt Maßstäbe

Gesetz zur Förderung der digitalen Verwaltung

Wichtige Signale zu Gunsten des Datenschutzes sendete – nicht zum ersten Mal – der Europäische Gerichtshof (EuGH). So entschied er, dass die Betreiber einer Facebook-Fanpage neben dem amerikanischen Unternehmen selbst ebenfalls im datenschutzrechtlichen Sinn als „Verantwortliche" zu werten sind. In einem Gutachten legte der EuGH zudem wichtige Maßstäbe für die Nutzung von Fluggastdaten fest.

## Kontrovers diskutierte Gesetzentwürfe

Neue Befugnisse für die Polizei

Wie schon in den Jahren zuvor, war ich auch im Zeitraum dieses Tätigkeitsberichts in die Debatten um neue Gesetzesvorhaben in Niedersachsen eingebunden. Besonders erwähnen möchte ich hier zum einen das „Gesetz zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes". Es soll Verwaltungsmodernisierung und Bürokratieabbau fördern und die Grundlage für eine moderne IT-Sicherheitsarchitektur in der niedersächsischen Verwaltung schaffen. Allerdings sieht der Gesetzentwurf weitreichende Eingriffsbefugnisse vor. Ich habe deshalb an verschiedenen Stellen deutliche Nachbesserungen zum Schutz der Betroffenen gefordert.

Datenschutz-Defizite bei der Überwachung und in den Leitstellen

Zum anderen brachten die Regierungsfraktionen im Mai 2018 ein Reformgesetz zum Gefahrenabwehrrecht in den Landtag ein. Dieses sah zahlreiche neue Befugnisse zur Datenerhebung für die Polizei vor, von denen einige tief in die Privatsphäre der Bürger eingreifen. Daher habe ich auch an diesem Entwurf teils scharfe Kritik geäußert.

## Erhebliche Mängel bei der Polizei

Überhaupt nahm der Datenschutz bei Polizei und Sicherheitsbehörden wieder breiten Raum in der Arbeit meines Hauses ein. So beschäftigten mich erneut die erheblichen Mängel im technisch-organisatorischen Datenschutz bei der polizeilichen Telekommunikationsüberwachung. Auch Ende 2018 sind diese bedauerlicherweise immer noch vorhanden.

Anlass zur Sorge bot ebenso der Umgang mit personenbezogenen Daten in den Leitstellen der Polizei. Obwohl sie teils hochsensible Daten verarbeiten, hielten sich die Leitstellen über Jahre nicht an die datenschutzrechtlichen Vorgaben. Inzwischen ist hier allerdings Besserung in Sicht. Weiterhin kritisch sehe ich dagegen die Verwendung des Messenger-Dienstes NIMes auf privaten Endgeräten der Polizeibeamten.

## Sensible Daten im Schul- und Gesundheitsbereich

Besonders im Fokus von Datenschützern sind immer wieder hochsensible Daten, etwa die von Patienten oder Kindern und Jugendlichen. Entsprechend deutlich habe ich mich zur Verwendung des Messenger-Dienstes „WhatsApp" im schulischen Bereich positioniert. Ich betrachte es als unzulässig, wenn Lehrkräfte untereinander oder mit den Schülern und deren Erziehungsberechtigten auf diesem Weg kommunizieren. Darüber habe ich die Schulen direkt mithilfe eines Merkblatts informiert. Informationsblätter mit gleich lautendem Tenor habe ich auch für die Nutzung von WhatsApp in Unternehmen und in Behörden veröffentlicht.

WhatsApp in Schulen unzulässig

Meine Position zu WhatsApp bedeutet allerdings nicht, dass ich der Digitalisierung in Schulen grundsätzlich kritisch gegenüber stehe. Sie muss zweifellos weiter vorangetrieben werden, allerdings unter Einhaltung der datenschutzrechtlichen Vorschriften. So sollten etwa bei der in Niedersachsen geplanten Bildungscloud Datenschutz und -sicherheit besondere Aufmerksamkeit genießen. Daher habe ich gefordert, mein Haus frühzeitig in die Entwicklung einzubinden. Doch ein prüfbares Datenschutzkonzept konnte mir bis jetzt nicht vorgelegt werden.

Dass es auch anders geht, zeigte meine Prüfung der niedersächsischen Gesundheitsregionen. Die in diesem Bericht beschriebenen Projekte machen deutlich, dass selbst im datenschutzrechtlich sensiblen Gesundheitsbereich innovative Projekte nach wie vor möglich sind, ohne gegen geltendes Recht zu verstoßen. Ebenfalls erfreulich ist es, dass es gelungen ist, die Tätigkeit des juristischen Kompetenzzentrums im Maßregelvollzug – zumindest im zweiten Anlauf – datenschutzgerecht zu gestalten.

Positives Beispiel Gesundheitsregionen

## Datenschutz auf Rädern

Ein weiterer Erfolg für den Datenschutz betrifft des Deutschen liebstes Kind – sein Auto. Im Zeitraum dieses Berichts haben die Datenschutzaufsichtsbehörden mit dem Verband der Automobilindustrie ein Musterkapitel „Datenschutz" für die Betriebsanleitung im Autocockpit erarbeitet. Dieses soll in sämtlichen Fahrzeugen zahlreicher deutscher Hersteller Verwendung finden und so den Fahrer kompakt und transparent über die Datenströme seines Autos informieren.

Musterkapitel für die Kfz-Anleitung

Immer wieder haben auch Arbeitgeber Interesse an den Daten aus ihrem Fuhrpark. Mich erreichen deshalb häufig Beschwerden von Beschäftigten, dass ihre Firmenfahrzeuge von geortet werden können. Die Daten werden zum Teil genutzt, um die Beschäftigten zu kontrollieren, wogegen ich mehrfach vorgegangen bin. In diesem Bericht finden sich Beispiele dafür, wann die Ortung per GPS zulässig ist und wann nicht.

GPS-Ortung von Arbeitnehmern

Ebenfalls heikel ist nach wie vor die Verwendung von Dashcams im Straßenverkehr. In der Regel sind sie datenschutzrechtlich unzulässig. Das wurde auch in einem Klageverfahren deutlich, das „Knöllchen-Horst" gegen meine Behörde angestrengt hatte. Inzwischen gibt es zu diesem Thema ein Urteil des Bundesgerichtshofes.

Gestritten wird ebenfalls immer noch über den Kameraeinsatz im öffentlichen Nahverkehr. Per Anordnung wollte ich dem Verkehrsbetrieb ÜSTRA aufgeben, die Videoüberwachung in Bussen und Stadtbahnen einzustellen. Das Oberverwaltungsgericht Lüneburg sah die Kameras allerdings als zulässig an und ließ keine Revision gegen sein Urteil zu. Um diese wichtige Frage doch noch höchstrichterlich klären zu lassen, habe ich Nichtzulassungsbeschwerde beim Bundesverwaltungsgericht eingelegt.

Kontroverse über Kameras im ÖPNV

# C. Zahlen und Fakten

## Zahlen und Fakten

Transparenz ist für öffentliche Stellen stets ein erstrebenswertes Gut, so auch für die Datenschutzbehörden des Bundes und der Länder. In diesem Sinne fasste die Datenschutzkonferenz im November 2018 den Beschluss, künftig optional ein einheitlich strukturiertes Kapitel in die Tätigkeitsberichte aufzunehmen. In diesem sollen verschiedene statistische Werte und ressourcenbezogene Informationen veröffentlicht werden.

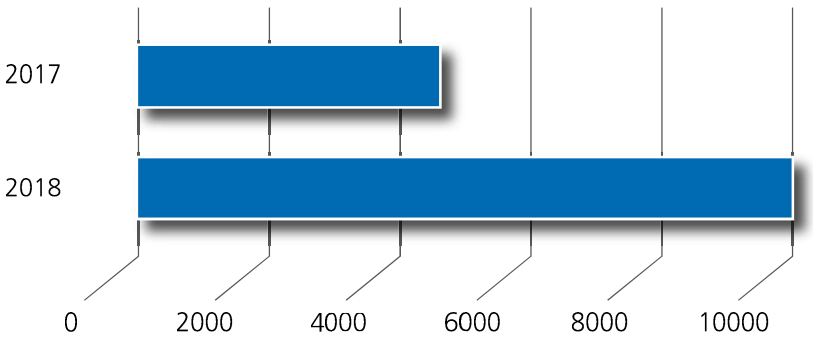
Das neue Kapitel soll u. a. Angaben zu Beschwerden, schriftlichen Beratungen, Meldungen von Datenschutzverletzungen, getroffenen Abhilfemaßnahmen, europäischen Verfahren und Ressourcen der Behörde enthalten. Ich werde dieses Kapitel ab dem Tätigkeitsbericht 2019 nach den Beschlüssen der Datenschutzkonferenz aufnehmen, möchte aber auch in diesem Bericht bereits einige wichtige Kennzahlen aufführen.

### Anfragen allgemein

Anfragen mehr als verdoppelt

Die Zahl der gesamten Anfragen, die meine Behörde erreichten, sei es telefonisch, schriftlich oder per E-Mail, erhöhte sich von ca. 4700 in 2017 auf 10.000 im Jahr darauf. Besonders in den Wochen rund um den Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) nahmen die Eingänge exponentiell zu.

Anfragen gesamt



## Beschwerden

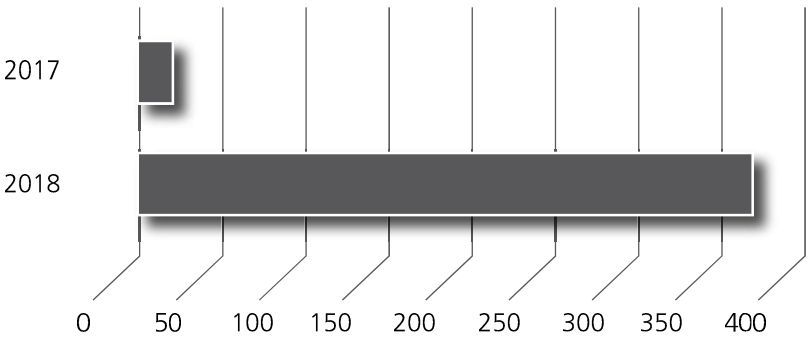
Gesondert erfasst werden Datenschutz-Beschwerden in meiner Behörde erst seit 2018. In diesem Jahr reichten mehr als 1000 Betroffene formell Beschwerde bei mir ein, weil sie sich in ihren Rechten verletzt fühlten.

## Gemeldete Datenschutzverletzungen

Meldepflicht deutlich verschärft

Die Pflicht zur Meldung einer Datenschutzverletzung wurde mit Geltung der DS-GVO erheblich verschärft. Dem entsprechend war es für mich wenig überraschend, dass sich die Meldungen enorm steigerten. Wurden meiner Behörde 2017 nur 20 sogenannte Datenpannen gemeldet, waren es 2018 bereits rund 370.

Datenschutzverletzungen



## Abhilfemaßnahmen nach DS-GVO

Schwerpunkt lag bisher auf Beratung

Die Datenschutz-Grundverordnung gesteht den Aufsichtsbehörden eine Reihe von Abhilfemaßnahmen zu, darunter Warnungen, Verwarnungen, Anordnungen und Geldbußen. 2018 habe ich den Schwerpunkt meiner Arbeit auf die Beratung zur DS-GVO gelegt und deshalb nur selten von diesen Maßnahmen Gebrauch gemacht. Verantwortliche sollten aber nicht davon ausgehen, dass das auch in Zukunft so sein wird. Insgesamt habe ich 2018 eine Warnung und 23 Verwarnungen nach Art. 58 Abs. 2 DS-GVO ausgesprochen.

## Ordnungswidrigkeiten-Verfahren und Bußgelder

Bußgelder werden meist akzeptiert

Im Berichtszeitraum habe ich 88 Bußgeldverfahren bearbeitet, in denen ich 25 Bußgelder über zusammen mehr als 36.000 Euro festgesetzt habe. Ganz überwiegend wurden die Bußgelder von den Adressaten akzeptiert und bezahlt. Die inhaltlichen Schwerpunkte bei den geahndeten Verstößen lagen im Bereich der unbefugten Videoüberwachung und der Nichterfüllung von Betroffenenrechten.
In neun Fällen habe ich Bußgelder gegen natürliche Personen festgesetzt. Die übrigen 16 Bußgelder habe ich gegenüber Unternehmen verhängt, bei denen mangelhafte organisatorische Strukturen oder Handlungen von Personen mit Leitungsaufgaben zum Verstoß führten.

Unrechtsgehalt und wirtschaftliche Verhältnisse fließen mit ein

Bei der Festsetzung des Bußgeldes fließen auch der Unrechtsgehalt und die wirtschaftlichen Verhältnisse des Adressaten ein. Das kann bei gleichgelagerten Sachverhalten zu deutlich unterschiedlichen Bußgeldhöhen führen. Zudem ist der eröffnete Bußgeldrahmen bei vorsätzlich begangenen Ordnungswidrigkeiten doppelt so hoch wie bei lediglich fahrlässigen Verstößen.
Sieben Bußgeldverfahren habe ich mit Verwarnungen ohne Verwarnungsgeld abgeschlossen. In diesen Fällen waren die datenschutzrechtlichen Verstöße so geringfügig, dass ich von der Festsetzung eines Bußgeldes absehen konnte.

Abgabe an die Staatsanwaltschaft

Wenn sich bei der Prüfung der Ordnungswidrigkeit der Anfangsverdacht einer Straftat ergibt, bin ich verpflichtet, den Vorgang an die zuständige Staatsanwaltschaft abzugeben. Das ist im Berichtszeitraum auch in einigen Fällen geschehen.

Die Staatsanwaltschaften haben in zahlreichen weiteren Verfahren festgestellt, dass ein datenschutzrechtlicher Straftatbestand nicht erfüllt war. Diese Verfahren wurden dann zur Durchführung eines Kontroll- oder Bußgeldverfahrens an mich abgegeben.
In drei Fällen habe ich einen eigenen Strafantrag nach § 44 BDSG gestellt.

Bußgelder nach DS-GVO werden höher ausfallen

Bußgelder nach DS-GVO habe ich im Berichtszeitraum nicht verhängt. Mit Geltung der Verordnung hat sich der Sanktionsrahmen allerdings um ein Vielfaches gesteigert. Ich gehe deshalb davon aus, dass ich in Zukunft weit höhere Bußgelder verhängen werde.

## Ressourcen der Behörde

Zur Bewältigung der Aufgaben und Umsetzung der Europäischen Datenschutzreform wurden meiner Behörde im Doppelhaushalt 2017/18 sieben Stellen zugesprochen. Diese wurden für fünf Juristen- und zwei Sachbearbeiterstellen eingesetzt. Zwei weitere Stellen, die im Doppelhaushalt

Neue Stellen für DS-GVO und Verwaltung

2017/18 enthalten waren, sind nicht auf die DS-GVO bezogen, sondern waren in der im Jahr 2011 erlangten Unabhängigkeit meiner Behörde begründet. Sie dienen dementsprechend der Erfüllung von Querschnittsaufgaben in der Verwaltung.

| Jahr | Budget in Tsd. Euro | Beschäftigungsvolumen |
|---|---|---|
| 2017 | 3.581 | 5,25 |
| 2018 | 3.917 | 50,25 |

# D. Entwicklungen im europäischen Datenschutz

## D.1. DS-GVO

### 1.1 Die DS-GVO kommt – Europa macht sich bereit für das neue Recht

Nicht ohne Grund gewährte der Gesetzgeber eine Übergangszeit von zwei Jahren bis zur Geltung der Datenschutz-Grundverordnung (DS-GVO). Diese umfassende Rechtsreform verlangte nicht nur von den datenverarbeitenden Stellen einige Vorbereitungen. Auch die Aufsichtsbehörden in der EU waren damit in den Jahren 2017 und 2018 beschäftigt: Hilfestellungen für die Datenverarbeiter zum neuen Recht waren zu erstellen, interne Verfahren zur Durchführung der neuen europäischen Kooperationsverfahren mussten installiert werden und schließlich war der neue Europäische Datenschutzausschuss (EDSA) aufzubauen.

#### Leitlinien – Hilfen für die Praxis

LfD wirkt in Arbeitsgruppen mit

Schon früh trugen die datenverarbeitenden Stellen an die Datenschutzaufsichtsbehörden den Wunsch heran, Auslegungshilfen für die neuen Regelungen zur Verfügung zu stellen. Die Art. 29-Gruppe (das europäische Gremium der Aufsichtsbehörden vor der DS-GVO) nahm deshalb die Erstellung von Leitlinien zur DS-GVO als weiteren Punkt in ihr Arbeitsprogramm für die Jahre 2016 bis 2018 auf. Die Leitlinien wurden von Unterarbeitsgruppen (Subgroups) der Art. 29-Gruppe erarbeitet. Durch aktive Mitwirkung in diesen Unterarbeitsgruppen hat auch meine Behörde an den Leitlinien mitgearbeitet und ihre Einflussmöglichkeit gewahrt.

Wichtige Bereiche, die viele Fragen bei den datenverarbeitenden Stellen aufwarfen, waren beispielsweise die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung (DSFA) oder das Recht auf Datenübertragbarkeit. Hierbei handelt es sich um neue Rechte bzw. um neu ausgestaltete Vorgaben. Auch zum betrieblichen Datenschutzbeauftragten traten viele Fragen auf, da dieser anders als in Deutschland für viele europäische Staaten weitgehend neu war.

Leitlinien können geändert und angepasst werden

Die Leitlinien stellen empfehlende Handlungsanweisungen dar. Sie sollen Hilfestellungen für die Anwendung des Rechts in der Praxis bieten. Dabei handelt es sich allerdings nicht um verbindliche Rechtssetzung – Leitlinien geben

die Auslegung bestimmter gesetzlicher Regelungen und Empfehlungen zur Anwendung durch die Aufsichtsbehörden wieder. Diese können daher gegebenenfalls angepasst und geändert werden, etwa aufgrund von neuer Rechtsprechung. Gerade im Anfangszeitraum eines neuen Gesetzes sind Leitlinien der Aufsichtsbehörden jedoch von besonderem Gewicht.

## Breites Themenspektrum

Zunächst wurden Leitlinien zu folgenden Themen verfasst: Datenübertragbarkeit, Datenschutzbeauftragte, Bestimmung der federführenden Aufsichtsbehörde und Datenschutzfolgenabschätzung.

Es folgten u.a. Leitlinien zur Meldung bei Datenschutzverletzungen und automatisierten Entscheidung im Einzelfall, zu Einwilligung und zu Transparenz. Weitere sind geplant, z. B. zu Privacy by Design und by Default sowie zu Verhaltungsregeln (Codes of Conduct).

Die Leitlinien enthalten jeweils Auslegungen unbestimmter Rechtsbegriffe, Beispiele und konkrete Handlungsempfehlungen für die Umsetzung in der Praxis. Jede Leitlinie wird nach Erstellung zunächst für sechs Wochen in die öffentliche Konsultation gegeben, in der Verbände, Unternehmen sowie gesellschaftliche Gruppen Kommentare und Änderungswünsche äußern können. So wird sichergestellt, dass die Leitlinien nicht an den Bedürfnissen der Anwender vorbei verfasst werden.

Leitlinien EDSA – Kurzlink: https://t1p.de/Leitlinien

Im Ergebnis haben die Aufsichtsbehörden damit Hilfestellungen für verschiedene Bereiche und Themen der DS-GVO verfasst und so zu einer einheitlichen Anwendung des neuen Rechts beigetragen. Mit der DS-GVO ist die Pflicht der Aufsichtsbehörden, durch den EDSA Leitlinien und Handlungsempfehlungen zum Datenschutzrecht zu erstellen, nun auch gesetzlich vorgesehen.

Die Leitlinien („Guidelines“) werden in englischer Sprache entworfen und abgestimmt. Die endgültige Fassung wird dann in alle Sprachen der EU-Mitgliedsstaaten übersetzt. Die jeweils englische Fassung der Guidelines und die deutschen Übersetzungen werden auf meiner Webseite bereitgestellt.

## Kurzpapiere der Datenschutzkonferenz

Bericht zu den Kurzpapieren der DSK auf Seite 23

Auf Bundesebene befasste sich die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) damit, Verantwortlichen praxisorientierte Handlungsempfehlungen zur Verfügung zu stellen. 19 Kurzpapiere dienen als erste Orientierungshilfe, wie die DS-GVO im praktischen Vollzug angewendet werden sollte. Die Papiere sind jedoch nicht als endgültig zu verstehen, sondern stehen unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Europäischen Datenschutzausschuss.

## Eine neue Institution – der Europäische Datenschutzausschuss

EDSA ersetzt Art. 29-Gruppe

Die ersten Leitlinien zur DS-GVO wurden noch von der Art. 29-Gruppe verabschiedet. Dieses Gremium wurde jedoch mit Inkrafttreten der DS-GVO aufgelöst und durch den Europäischen Datenschutzausschuss (EDSA) ersetzt. Der EDSA hat nun ein weitaus höheres Gewicht, welches in seinen gesetzlich zugewiesenen Aufgaben sichtbar wird.

Der Ausschuss ist nach der DS-GVO nicht nur dafür zuständig, zum Datenschutzrecht zu beraten, Leitlinien zu erstellen und Empfehlungen auszusprechen. Er wurde auch errichtet, um die

einheitliche Anwendung der DS-GVO in der Praxis zu gewährleisten. Dies ist als zentrale Aufgabe des neuen Gremiums anzusehen. Der EDSA ist streitentscheidende Stelle in Praxisfällen mit grenzüberschreitendem Bezug, wenn also mehrere Mitgliedstaaten der EU betroffen sind. Kommt es zwischen den Aufsichtsbehörden verschiedener Mitgliedstaaten nicht zu einer Einigung über ein einheitliches Vorgehen in einem konkreten Fall, entscheidet der EDSA endgültig und verpflichtend. Ebenso ist es seine Aufgabe, in abstrakten Streitfragen von hoher allgemeiner Bedeutung in den Mitgliedstaaten Vorgaben zu machen, die dann für alle Aufsichtsbehörden verbindlich zu beachten sind.

Entscheidende Instanz in Streitfällen

## Herausforderungen beim Aufbau des Ausschusses

Für die beteiligten Stellen bedeutete dies den Aufbau einer neuen Institution mit allen damit zusammenhängenden Herausforderungen. Da der EDSA ein gemeinsames Gremium der europäischen Aufsichtsbehörden ist, stand die Beteiligung Niedersachsens an den organisatorischen Vorarbeiten außer Frage. Die Aufsichtsbehörden waren also im Berichtszeitraum neben der Bearbeitung von Fachfragen auch mit Fragen zur Einrichtung des neuen EDSA befasst: Wie rekrutiert man fachkundige Beschäftigte, welches Budget ist angemessen, wie ist die IT-Fachanwendung auszugestalten, etwa im Hinblick auf die Zugangsberechtigung zu Dokumenten und auf Übersetzungsleistungen?

Fragen zu Ausstattung und Abläufen

Weiterhin war zu klären, wie die Sitzungen zu planen sind, wie die Öffentlichkeitsarbeit aussehen soll und wie die eigene Webseite des EDSA zu gestalten ist. Von besonderer Bedeutung war die Erarbeitung einer Geschäftsordnung. Darin geht es um Festlegungen zur konkreten Zusammenarbeit, zu Fristen, zum Verfahrensgang sowie zur verbindlichen Entscheidungsfindung.

Am Tag des Wirksamwerdens der DS-GVO, dem 25. Mai 2018, tagte auch der EDSA in seiner ersten Sitzung.

## Die europäischen Kooperationsverfahren

Das erstmalig eingeführte Prinzip des One-Stop-Shops und das vollkommen neue Kohärenzverfahren stellten auch die Aufsichtsbehörden vor neue Herausforderungen. Denn die DS-GVO verpflichtet die Aufsichtsbehörden in Europa zur Zusammenarbeit in Fällen mit grenzüberschreitender Bedeutung und gibt dabei ganz konkrete Verfahren vor. Immer dann, wenn von einer Entscheidung in einem Einzelfall mehrere Mitgliedstaaten betroffen sind, ist ein konkretes Verfahren der Zusammenarbeit und gegenseitigen Abstimmung über die Entscheidung vorgesehen.

Abstimmung bei grenzüberschreitenden Verfahren

Diese vorgesehen Verfahren bedurften einer Konkretisierung hinsichtlich ihres genauen Ablaufs: Welche Aufsichtsbehörde wird wann wie tätig, wann und wie werden die anderen betroffenen Aufsichtsbehörden eingebunden, welche Dokumente werden wie übersandt, wie geht man mit der Sprachbarriere um? Mit diesen Fragen beschäftigten sich die Aufsichtsbehörden in Vorbereitung auf die DS-GVO und einigten sich schließlich auf konkrete Verfahrensabläufe. So entstanden Handlungsanweisungen für die Verfahren der Kooperation und zum Dringlichkeitsverfahren.

Kooperation zwischen den Behörden

Die Kooperationsverfahren bedeuten in der Praxis eine umfangreiche Kommunikation zwischen den europäischen Aufsichtsbehörden in vielen Fällen. Es wurde also eine IT-Plattform gesucht, welche in der gesamten EU funktioniert und mit der ein Austausch unkompliziert und schnell möglich ist. Die europäischen Aufsichtsbehörden entschieden sich schließlich, das bereits auf EU-Ebene bestehende Internal Market Information System (IMI) zu nutzen. Dieses wurde für den Austausch von Datenschutz-Fällen gemäß den Ansprüchen der Aufsichtsbehörden fit gemacht, indem für die verschiedenen Verfahrensarten Formulare und Vorgehensweisen hinterlegt wurden. Die Aufsichtsbehörden erhielten schließlich Zugang für die Nutzung, Anwenderschulungen und eine umfangreiche Handlungsanleitung. Über das IMI-System wird heute eine Vielzahl von Fällen bearbeitet.

## Integration in die Behörde

Werden so umfangreiche neue Verfahren durch Gesetz vorgegeben, müssen diese auch in den Behörden-Ablauf eingebettet werden. Auch meine Behörde sah sich dabei völlig neuen Anforderungen gegenüber wie der regelmäßigen Kommunikation mit anderen Aufsichtsbehörden in englischer Sprache, der technischen Verfahrensabwicklung über das neue IMI-System und den neue Fristen zur Bearbeitung.

Vorabprüfung jeder Beschwerde nötig

Neu ist auch die regelmäßige Vorabprüfung jeder eingehenden Beschwerde, ob es sich um einen grenzüberschreitenden Fall handelt und ob daraufhin das Kooperationsverfahren innerhalb der EU durchzuführen ist. Meine Behörde hat daher schon früh begonnen, sich auf diese neuen Herausforderungen einzustellen. Unter anderem wurde beschlossen, einen Übersetzungsdienst einzuschalten, um die sprachliche Richtigkeit unserer Entscheidungen und Stellungnahmen zu gewährleisten.

Neue Stelle zur Koordination

Zudem habe ich einen neuen zentralen Dienstposten in meinem Haus eingerichtet, der als zentrale Kontaktstelle für die europäischen Kooperationsverfahren agiert. Diese Stelle koordiniert sämtliche Verfahren, welche meine Behörde in Zusammenarbeit mit den anderen europäischen Aufsichtsbehörden führt. So ist sichergestellt, dass die Verfahren korrekt und einheitlich im IMI-System bearbeitet werden, Fristen eingehalten werden und wir unsere Beteiligung an uns betreffenden Verfahren gewährleisten können.

Die Erfahrung der vergangenen Monate hat gezeigt, dass diese Konzentrierung der Verfahren mit europäischem Bezug viele Vorteile hat. Einerseits werden die Fachreferate von englischsprachigen Eingängen und der ständigen Beobachtung des Verfahrensganges entlastet und können sich auf die inhaltliche Bearbeitung konzentrieren. Andererseits können die Verfahren trotz der großen Anzahl der im IMI-System behandelten Fälle bewältigt werden, weil eine systematische Einordnung schon bei Eingang der Fälle erfolgt, diese von zentraler Stelle übersetzt werden und ein allgemeiner Überblick über den Verfahrensstand in jedem Fall möglich ist.

# 1.2 Aktivitäten der Datenschutzkonferenz: Kurzpapiere zur DS-GVO

Breiten Raum in der Konferenz der Datenschutzbehörden von Bund und Ländern (DSK) nahm in meiner Vorsitzzeit die Datenschutz-Grundverordnung ein. Mit vielseitigen Maßnahmen und Initiativen bereitete die DSK die Geltung der Verordnung vor. In der Zeit meines Vorsitzes im Jahr 2017 wandte sich die DSK mit ihren Veröffentlichungen direkt an die verantwortlichen Stellen.

Mit verschiedenen Kurzpapieren stellte die Datenschutzkonferenz besonders den Verantwortlichen in der Wirtschaft bereits vor Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) praxisorientierte Handlungsempfehlungen zur Verfügung. Diese dienen als erste Orientierungshilfe, wie die DS-GVO im praktischen Vollzug angewendet werden sollte. Die 19 Papiere sind jedoch nicht als endgültig zu verstehen, sondern stehen unter dem Vorbehalt einer zukünftigen – möglicherweise abweichenden – Auslegung durch den Europäischen Datenschutzausschuss.

## Wertvolle und dringend notwendige Hilfe

Die hohe Nachfrage aus Unternehmen aber auch aus Verbänden und Vereinen zeigte, dass die Datenschutzkonferenz an dieser Stelle wertvolle und dringend notwendige Hilfestellung anbot. Denn die Verunsicherung angesichts des neuen europäischen Rechts war und ist groß – trotz der eingeräumten zweijährigen Übergangsfrist bis zur tatsächlichen Anwendung.

Kurzpapiere der DSK – Kurzlink: https://t1p.de/Kurzpapiere

Durch die Kurzpapiere standen den Verantwortlichen deutschlandweit einheitliche Auslegungen zur Verfügung, mit denen sowohl Unternehmen als auch Vereine ihre Datenverarbeitungsprozesse an die DS-GVO anpassen konnten. Und zwar bereits im Vorfeld der Anwendung der DS-GVO. Die DSK wird diesen Informationspool weiter ausbauen.

Nach Geltungsbeginn der DS-GVO sollen die zwangsläufig abstrakt gehaltenen Kurzpapiere dann langfristig durch Erfahrungen in der praktischen Anwendung ersetzt werden. Bis dahin werden sie fortlaufend aktualisiert.

# 1.3 Neu nach DS-GVO:

## Muss-Listen für Datenschutz-Folgenabschätzungen

Wenn Verantwortliche hochriskante Verfahren betreiben wollen, müssen sie vorab eine Datenschutz-Folgenabschätzung (DSFA) erstellen. Die Muss-Liste der zuständigen Datenschutz-Aufsichtsbehörde ist bei der Identifikation dieser hochriskanten Verfahren ein wichtiger Prüfungspunkt und gibt Orientierung.

Verantwortliche müssen sich mit Risiken auseinandersetzen

Die Datenschutz-Grundverordnung (DS-GVO) stellt besondere Anforderungen an Verarbeitungsvorgänge, bei denen ein hohes Risiko für die betroffenen Personen besteht. Eine DSFA soll gewährleisten, dass die Verantwortlichen sich umfangreich mit den Risiken für die betroffenen Personen auseinandersetzen, diese mit entsprechenden technischen und organisatorischen Maßnahmen reduzieren und einen Nachweis hierüber führen.

## Bundesweit einheitliche Maßstäbe

Im ersten Schritt müssen die Verantwortlichen zunächst identifizieren, ob sie hochriskante Verfahren betreiben und um welche es sich dabei handelt. Die Aufsichtsbehörden haben gemäß DS-GVO die Aufgabe, Listen mit entsprechenden Verfahren zu erstellen.

Dieser Aufgabe habe ich mich im nicht-öffentlichen Bereich gemeinsam mit meinen Kolleginnen und Kollegen in der Datenschutzkonferenz angenommen. Ziel war es, zunächst deutschlandweit einheitliche Maßstäbe zu entwickeln und anzuwenden, um den hier ansässigen Unternehmen eine verlässliche Basis zu bieten. Orientiert haben wir uns dabei an den Leitlinien zur Identifikation von hochriskanten Verfahren des Europäischen Datenschutzausschusses (EDSA).

## Wenig Anpassungsbedarf bei deutscher Liste

Im Ergebnis hat die Datenschutzkonferenz eine gemeinsame Liste für den nicht-öffentlichen Bereich beschlossen und diese anschließend dem EDSA vorgelegt. Dies ist gesetzlich vorgesehen und dient der einheitlichen Anwendung des Datenschutzrechts in der EU.

Der Ausschuss hat sowohl die deutsche Muss-Liste als auch die Listen der anderen Mitgliedsstaaten geprüft und Stellungnahmen[1] abgegeben. So konnte auch EU-weit eine weitgehende Harmonisierung bei den Muss-Listen erreicht werden. Erfreulich war, dass die deutsche Liste nur in geringem Umfang angepasst werden musste. Für die niedersächsischen Behörden und öffentlichen Stellen in meinem Zuständigkeitsbereich habe ich ebenfalls eine entsprechende Liste veröffentlicht.

Muss-Listen – Kurzlink: https://t1p.de/Muss-Listen

1 Stellungnahme zur deutschen Muss-Liste: Opinion 5/2018 on the draft list of the competent supervisory authorities of Germany regarding the processing operations subject to the requirement of data protection impact assessment (Article 35.4 GDPR), abrufbar auf https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52018-germany-sas-dpia-list_en

# 1.4 Die Grenzen der Harmonisierung – das neue Bundesdatenschutzgesetz

Im Mai 2016 trat die Datenschutzgrundverordnung (DS-GVO) in Kraft. Nun war der nationale Gesetzgeber an der Reihe – es galt, die Regelungsaufträge und Öffnungsklauseln der DS-GVO in deutsches Recht umzusetzen. Das im Jahr 2017 verabschiedete neue Bundesdatenschutzgesetz (BDSG) bedeutete aber leider einen Rückschritt gegenüber dem früheren Datenschutzniveau und sogar einen Verstoß gegen die Vorgaben der DS-GVO.

Datenverkehr erleichtern, Binnenmarkt stärken

Der europäische Gesetzgeber verfolgte mit der Reform auf EU-Ebene vor allem das Ziel, das Datenschutzrecht in der gesamten Union zu harmonisieren. In allen Mitgliedstaaten sollen grundsätzlich dieselben Regelungen für den Umgang mit personenbezogenen Daten gelten. Dies soll den freien Datenverkehr erleichtern, den Binnenmarkt in der EU stärken und auch verhindern, dass Unternehmen den Sitz ihrer Hauptniederlassung anhand vermeintlich schwächerer nationaler Regelungen zum Datenschutz festlegen.

## Wie groß ist der nationale Spielraum?

Dieses Ziel der Vereinheitlichung hat der Gesetzgeber mit der DS-GVO grundsätzlich erreicht. Allein durch die Rechtsform der Verordnung und die damit verbundene unmittelbare Geltung der neuen Regelungen in allen Mitgliedstaaten kann man von einem einheitlichen Datenschutzrecht in der EU sprechen.

Nicht überall abschließende Regelungen

Allerdings trifft auch die DS-GVO nicht in allen Bereichen abschließende Regelungen. Durch Öffnungsklauseln und Regelungsaufträge wird dem nationalen Gesetzgeber ein gewisser Spielraum für eigene Vorgaben eröffnet. Letztlich ist dies der Kern des Problems: Wie groß ist dieser Spielraum?

## Öffnungsklauseln und Regelungsaufträge

Öffnungsklauseln geben dem nationalen Gesetzgeber die Möglichkeit, in bestimmten Bereichen eigene Regelungen zu schaffen. Die DS-GVO erlaubt dies zum Beispiel für die Datenverarbeitung öffentlicher Stellen oder bei der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten. Regelungsaufträge müssen dagegen in nationales Recht umgesetzt werden. In der DS-GVO findet man diese zum Beispiel bei der Errichtung von Aufsichtsbehörden.

Nationaler Spielraum ist beschränkt

Vor diesem Hintergrund kann man durchaus Zweifel haben an einer vollständigen Harmonisierung des europäischen Datenschutzrechts. Doch sind die Regelungsmöglichkeiten auf nationaler Ebene beschränkt. Die DS-GVO ist immer als übergeordnetes Regelwerk bindend, der Spielraum des nationalen Gesetzgebers ist daher eng auszulegen und nur begrenzt zu nutzen.

## Keine Wiederholungen und Hintertür-Gesetze

Keine Senkung des Schutzniveaus

Bei der Umsetzung europäischer Rechtsetzung in nationales Recht ist daneben zu beachten, dass bestehende Regelungen nicht einfach wiederholt werden dürfen und dass das nationale Recht nicht zu einer Senkung des durch die DS-GVO vorgegebenen Datenschutzniveaus führen darf. Insbesondere dürfen auf diesem Weg nicht Regelungen durch die Hintertür verabschiedet werden, welche im vorherigen Gesetzgebungsverfahren auf EU-Ebene nicht durchgesetzt werden konnten.
Das neue BDSG verstößt gegen diese Grundsätze.

## Neues Gesetz senkt Standards

Anfang 2017 gab das Bundeskabinett zunächst seinen finalen Entwurf des neuen BDSG bekannt. Es stellt ergänzende bzw. einschränkende Regelungen für öffentliche Stellen des Bundes und für private Datenverarbeiter zu folgenden Bereichen auf:

Regelungen des neuen BDSG

- Generalklausel zur Verarbeitung personenbezogener Stellen durch öffentliche Stellen
- Videoüberwachung
- Benennung von Datenschutzbeauftragten
- Bundesbeauftragte(r) für den Datenschutz (BfDI)
- Vertretung im Europäischen Datenschutzausschuss (EDSA) und Zusammenarbeit der Aufsichtsbehörden
- Verarbeitung besonderer Kategorien personenbezogener Daten
- Weiterverarbeitung zu Sekundärzwecken
- Datenverarbeitung im Beschäftigungsverhältnis
- Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken
- Berufsgeheimnisträger
- Einschränkung der Betroffenenrechte
- Sanktionen
- Umsetzung der Richtlinie für Polizei und Justiz

## Niedrigeres Schutzniveau befürchtet

Genutzter Spielraum nicht akzeptabel

Die Regelungsaufträge und Öffnungsklauseln wurden damit grundsätzlich umgesetzt. Umfang und Inhalt der Umsetzung und Nutzung des Spielraums der DS-GVO waren jedoch in diesem Entwurf in großen Teilen nicht akzeptabel. Es stand zu befürchten, dass im neuen BDSG europarechtswidrige Normen festgeschrieben werden und Regelungen getroffen werden, die zu einer Absenkung des Datenschutzniveaus führen bzw. dass unscharfe Regelungen Unsicherheiten in der Praxis auslösen.

Änderungsanträge der DSK

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) erarbeitete daher im Rahmen der Bundesratsbefassung zum BDSG konkrete Änderungsanträge:

- Vertretung der Bundesländer im EDSA: Im Ausschuss sollte nicht nur die BfDI die deutschen Interessen vertreten, sondern aufgrund der eindeutigen Zuständigkeitsverteilung in der Sache auch ein Vertreter der Länder-Aufsichtsbehörden teilnehmen.
- Betroffenenrechte: Der vorliegende Entwurf des BDSG sah zu starke Einschränkungen der Betroffenenrechte vor, obwohl die DS-GVO gerade diese Rechte stärkt.
- Verarbeitung besonderer Kategorien von personenbezogenen Daten: Der vorliegende Erlaubnistatbestand gestattete viel zu weitgehend und insbesondere ohne Erfordernis einer Interessenabwägung im Einzelfall die Verarbeitung dieser besonders sensiblen Daten.
- Berufsgeheimnisträger: Der Entwurf versagte den Aufsichtsbehörden die Kontrollbefugnis über Berufsgeheimnisträger wie Rechtsanwälte, obwohl gerade in diesem Bereich eine Verarbeitung besonders sensibler Daten stattfindet.
- Videoüberwachung: Die Erlaubnis zur Videoüberwachung durch Private war viel zu weitgehend und beruhte nicht auf einer Öffnungsklausel der DS-GVO.

## Gesetz mit Mängeln verabschiedet

Nur wenige Forderungen werden umgesetzt

Die DSK hatte leider nur mit einigen wenigen dieser Änderungsanträge Erfolg, nämlich:

- Auch die Aufsichtsbehörden der Bundesländer entsenden nun einen eigenen Vertreter in den EDSA.
- Die sehr weitgehende Einschränkung der Betroffenenrechte wurde teilweise zurückgenommen.

- Hinsichtlich der Verarbeitung besonders sensibler personenbezogener Daten wurden die ausufernden Erlaubnistatbestände durch die Ergänzung einer Pflicht zur Interessenabwägung im Einzelfall eingeschränkt.

Die Forderungen nach einer Kontrollbefugnis der Aufsichtsbehörden für Berufsgeheimnisträger und zu einer Einschränkung der Erlaubnis zur Videoüberwachung im Rahmen der DS-GVO blieben dagegen ohne Erfolg. Am 3. Juli 2017 wurde das neue BDSG mit diesen weiter bestehenden Mängeln beschlossen.

## Zweifel an Konformität mit Europarecht

Im Ergebnis liegt nun ein BDSG vor, das tatsächlich eine Senkung des bisher bestehenden Datenschutzniveaus darstellt und darüber hinaus den Vorgaben der DS-GVO widerspricht. Es steht zu befürchten, dass dieses BDSG in Teilen europarechtswidrig ist.

Einschränkung der Betroffenenrechte

Insgesamt ist eine fehlerhafte Anwendung und Auslegung der vorhandenen Regelungsaufträge und Öffnungsklauseln der DS-GVO zu beklagen. Als Beispiel sei die Öffnungsklausel in Art. 23 DS-GVO genannt, welche nationale Einschränkungen der Betroffenenrechte ermöglicht, wo diese notwendig und verhältnismäßig sind. Die Einschränkungen der Rechte auf Information oder Auskunft der betroffenen Person im BDSG dienen nun allerdings offenkundig lediglich der Arbeitserleichterung für die Daten verarbeitenden Stellen. Bedenkt man, wie wesentlich die Betroffenenrechte im Datenschutz sind – zur Kontrolle über die eigenen personenbezogenen Daten – sind solche Ausnahmen nicht akzeptabel.

## Keine Öffnungsklausel zur Videoüberwachung

DSK fordert Gesetz zum Datenschutz von Beschäftigten

Daneben verstößt das neue BDSG an verschiedenen Stellen gegen das Wiederholungsverbot, indem Regelungen der DS-GVO einfach übernommen werden, ohne diese zu konkretisieren. Dies zeigt sich zum Beispiel in den wenigen inhaltsleeren Bestimmungen zum Beschäftigten-Datenschutzrecht. Die DSK hatte hier mehrfach ein eigenes Beschäftigtendatenschutzgesetz gefordert, für welches die DS-GVO auch eine eigene Öffnungsklausel bereithält.

Am deutlichsten wird das Versagen des deutschen Gesetzgebers bei der Videoüberwachung durch private Stellen. Die DS-GVO regelt umfassend sämtliche Aspekte des Datenschutzes und eröffnet daneben in einigen wenigen Bereichen die Möglichkeit zu nationalen Regelungen. Diesen Grundsatz hat der deutsche Gesetzgeber ignoriert und trotz fehlender Öffnungsklausel in diesem Bereich eigene Bestimmungen zur Videoüberwachung durch Private getroffen.

Neues BDSG verstärkt die Rechtsunsicherheit

Das neue BDSG untergräbt die Bemühungen des europäischen Gesetzgebers um ein besseres Datenschutzrecht. Es ist bedauerlich, dass gerade in Deutschland mit seinem traditionell hohen Datenschutzniveau nun Standards in Frage gestellt werden. Zudem verstärkt das BDSG die Rechtsunsicherheit, da an vielen Stellen Zweifel an der Europarechtskonformität bestehen. Damit stehen die Datenschutzaufsichtsbehörden vor der enormen Herausforderung, die entsprechenden Regelungen im BDSG in der konkreten Fallbearbeitung soweit wie irgend möglich europarrechtskonform auslegen zu müssen.

# 1.5 Neues niedersächsisches Datenschutzgesetz für Behörden

Spätestens mit Inkrafttreten der Datenschutz-Grundverordnung am 25. Mai 2016 war klar, dass der Landesgesetzgeber das niedersächsische Datenschutzgesetz grundlegend überarbeiten muss. Zu meinem Bedauern fand die parlamentarische Beratung dazu unter hohem Zeitdruck statt. Wichtige Forderungen aus meinem Haus blieben letztlich unberücksichtigt.

Forderung: Hohes Datenschutzniveau aufrecht erhalten

Einen ersten Referentenentwurf zur Änderung des niedersächsischen Datenschutzgesetzes (NDSG) legte das Innenministerium im März 2017 vor. Zu diesem nahm meine Behörde ausführlich Stellung. Besonders mahnte ich an, das hohe Datenschutzniveau innerhalb der öffentlichen Verwaltung aufrechtzuerhalten. Zudem forderte ich ein Datenschutzrecht für alle Behörden, also auch für Polizei-, Gefahrenabwehr und Justizbehörden, normiert in einem Gesetzeswerk. Der Referentenentwurf sah allerdings die Umsetzung der Richtlinie vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum Zweck der Verhütung, Ermittlung Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung (sog. JI-Richtlinie) nicht vor.

## Überarbeiteter Entwurf nach der Neuwahl

80 Hinweise zum neuen Entwurf

Die vorgezogenen Landtagswahlen in Niedersachsen sorgten dafür, dass erst im Oktober 2017 die Arbeiten am Gesetzentwurf wieder aufgenommen wurden. Die neue Landesregierung beschloss umgehend, einen überarbeiteten Entwurf zur Verbandsbeteiligung frei zu geben. Zu diesem Entwurf, der auch die Anpassung zahlreicher Fachgesetze vorsah, nahm meine Behörde wiederum ausführlich mit mehr als 80 Hinweisen Stellung. So konnte der Gesetzentwurf aus Sicht des Datenschutzes an zahlreichen Stellen wesentlich verbessert werden. Unter anderem wurde Folgende geändert:

- Aufnahme einer Regelung zur Datenverarbeitung für automatisierte Abrufverfahren und gemeinsame Dateien.
- Stärkere Verankerung der Dokumentationspflicht bei der Beschränkung von Rechten der betroffenen Person in einem gesonderten Paragrafen, insbesondere wenn die Behörde das grundsätzlich bestehende Auskunftsrecht einschränken will.
- Begrenzung der Speicherung von Bildmaterial im Rahmen einer Videoüberwachung auf höchstens drei Wochen. Vorher gab es keine Speicherbegrenzung.
- Grundlegende Überarbeitung der Regelung zur Datenverarbeitung zu Forschungszwecken sowie der Tatbestände für Ordnungswidrigkeiten und Straftaten.

- Verankerung des uneingeschränkten Auskunftsrechts der Landesbeauftragten, wenn eine Behörde die Auskunft gegenüber dem Bürger verweigert. Die Behörde muss dann gegenüber der Landesbeauftragten den Datenverarbeitungsvorgang offen legen, so dass die Rechtmäßigkeit für den Bürger überprüft werden kann.

Umsetzung der JI-Richtlinie

Die Landesregierung hat sich mit dem neuen Datenschutzgesetz im März 2018 erneut befasst, um dieses nach der Verbandsbeteiligung in den Landtag einzubringen. Zeitgleich legten die Regierungsfraktionen einen weiteren Gesetzentwurf vor, der die Bestimmungen der JI-Richtlinie umsetzen sollte.[1] Beide Entwürfe wurden im weiteren parlamentarischen Verfahren miteinander verbunden, um ein Datenschutzrecht zu erhalten, das die Datenverarbeitung für alle Behörden in Niedersachsen in einem Gesetzeswerk regelt. Damit wurde eine wichtige Forderung meiner Behörde in letzter Minute umgesetzt.

Anhörungsergebnisse nicht ausreichend diskutiert

Bedauerlicherweise fanden die weiteren parlamentarischen Beratungen unter hohem Zeitdruck statt. Die Ergebnisse der Anhörung im Innenausschuss vom 27. April 2018 konnten daher nicht im ausreichenden Maße diskutiert werden. Schon am 16. Mai 2018 wurde das Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts im Landtag verabschiedet.

## Wichtige Vorschläge bleiben unbeachtet

Wichtige datenschutzrechtliche Forderungen meiner Behörde blieben damit unberücksichtigt. Dies betraf u. a. die Regelungen zur Videoüberwachung in § 14 NDSG, die eine uferlose Ausweitung der selben befürchten lassen. Denn der Zweck der Überwachung ist nicht mehr wie bisher auf die Ausübung des Hausrechts oder auf den Schutz von Personen und Sachen beschränkt. Auch fehlen Regelungen zur Vollstreckbarkeit meiner Anordnungen gegenüber Behörden, wenn diese gegen datenschutzrechtliche Vorschriften verstoßen. Anders als bei Wirtschaftsunternehmen können in diesen Fällen auch keine Bußgelder verhängt werden. Damit bleibt das neue NDSG hinter den Vorgaben der DS-GVO zurück, denn dort werden den Aufsichtsbehörden umfassende und wirksame Abhilfebefugnisse eingeräumt, wenn verantwortliche Stellen gegen den Datenschutz verstoßen.

Keine wirksamen Befugnisse gegenüber Behörden

Trotz der verkürzten Beratungen im parlamentarischen Verfahren wurden einige wenige aber wichtige Anregungen meiner Behörde aufgegriffen. So ist unbeschadet von spezielleren Fachgesetzen nun ausdrücklich geregelt, unter welchen Voraussetzungen Behörden personenbezogene Daten übermitteln dürfen (§ 5 Abs. 1 NDSG). Auch über die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten findet sich nun eine gesonderte Regelung (§ 17 NDSG).

Weitere Novelle notwendig

Die Landesregierung muss mit Blick auf die zügige Verabschiedung des Gesetzes und die unzureichende Beratung kritisch in den Blick nehmen, ob der Datenschutz in Niedersachsen tatsächlich umfassend alltagstauglich für die Behörden geregelt ist. Insbesondere muss noch einmal in allen Geschäftsbereichen geprüft werden, ob in den zahlreichen landesrechtlichen Vorschriften alle notwendigen Anpassungen vorgenommen wurden, die für eine der DS-GVO entsprechende Verarbeitung personenbezogener Daten erforderlich sind.

1 Vgl. hierzu den gesonderten Bericht zur Umsetzung der JI-Richtlinie auf Seite 37.

## 1.6 Folgen der DS-GVO für das nationale Medienprivileg

Die Datenschutz-Grundverordnung verfolgt das Ziel, das europäische Datenschutzrecht zu vereinheitlichen. Dieser Ansatz bringt es mit sich, dass nationale Sonderregelungen angepasst werden müssen. So auch das Medienprivileg, das in Deutschland in verschiedenen Gesetzen geregelt ist und für die Presse, den öffentlich-rechtlichen und privatrechtlichen Rundfunk sowie für Anbieter von Telemedien mit journalistisch-redaktionell gestalteten Angeboten gilt.

### Ausgleich zwischen Datenschutz und Pressefreiheit

Das Medienprivileg entband die aufgeführten Medien weitgehend von den nationalen Datenschutzvorschriften bei der Verarbeitung von personenbezogenen Daten zu journalistischen Zwecken. Erforderlich sind diese Ausnahmen, um einen Interessenausgleich zwischen der informationellen Selbstbestimmung einerseits sowie der Presse- und Rundfunkfreiheit andererseits zu erzielen. Mit dem Medienprivileg hat der Gesetzgeber grundsätzlich der gesellschaftlich bedeutsamen Presse- und Rundfunkfreiheit den Vorrang vor der im individuellen Interesse zu gewährleistenden informationellen Selbstbestimmung gewährt.

## Spielraum für Bundes- und Landesgesetzgeber

Bis zur Datenschutz-Grundverordnung (DS-GVO) gab es für die Regelung des Medienprivilegs keine konkreten Vorgaben aus Europa. Art. 85 DS-GVO hat hier eine entscheidende Änderung herbeigeführt. Die DS-GVO selbst regelt keine Ausnahmen für die journalistische Tätigkeit, sondern räumt den Mitgliedstaaten diesbezüglich einen Regelungsspielraum ein. Ausnahmenvorschriften und Abweichungen von der DS-GVO sind aber nur unter den folgenden Voraussetzungen zulässig:

Voraussetzungen für Ausnahmen von der DS-GVO

1. Es sind nicht von allen Vorschriften der DS-GVO Ausnahmen zulässig, sondern explizit nur von den Kapiteln II, III, IV VI, VII und IX.

2. Sie dürfen nur für die Verarbeitung von personenbezogenen Daten zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken vorgenommen werden.

3. Sie müssen erforderlich sein, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

## Gesetzentwürfe missachten die DS-GVO

Entschließungen der DSK: – Kurzlink: https://t1p.de/DSKEntschliessungen

Erste Gesetzentwürfe zur Anpassung des Medienprivilegs an die DS-GVO hatten diese Vorgaben überwiegend missachtet. Die Konferenz der deutschen Aufsichtsbehörden (DSK) fasste daher bereits am 9. November 2017 eine Entschließung zur Umsetzung der DS-GVO im Medienrecht. Darin wurden die nationalen Bundes- und Landesgesetzgeber nachdrücklich aufgefordert, die Vorgaben von Art. 85 DS-GVO einzuhalten. Dieser verbietet eine pauschale Aufhebung der Anwendbarkeit der Vorschriften der DS-GVO für Presse- und Rundfunkunternehmen. Es wurde betont, dass nur konkrete, spezifische und – vor allem – begründete Ausnahmen und Abweichungen von den Vorgaben der DS-GVO für die Datenverarbeitung zu journalistischen Zwecken erlaubt sind. Wie mir die weiteren Gesetzgebungsverfahren in Niedersachsen zeigten, ist dieser Appell jedoch leider weitgehend verhallt.

# 1.7 Organisatorische Anpassungen bei der Landesbeauftragten für den Datenschutz

Auch meine Behörde selbst musste sich intern auf die Neuerungen der Datenschutz-Grundverordnung (DS-GVO) einstellen. Ich nahm deshalb einige organisatorische Veränderungen vor – die umfassendste im Frühjahr 2018.

Fachthemen zentral bearbeiten

Knapp acht Wochen vor Geltungsbeginn der DS-GVO war es zum 1. April 2018 an der Zeit, Teile der Organisation und Geschäftsverteilung meiner Behörde anzupassen. Fachthemen wie Videoüberwachung, Datenschutzbeauftragte und Beschäftigtendatenschutz waren zuvor in verschiedenen Referaten getrennt nach öffentlichen und nicht-öffentlichen Stellen bearbeitet worden. Diese strikte Trennung war nun nicht mehr zeitgemäß, da die DS-GVO unmittelbar für öffentliche und nicht-öffentliche Stellen gilt. Im Zuge der Organisationsveränderung sollten diese Fachthemen deshalb ab sofort zentralisiert bearbeitet werden.

Sanktionen vom Wirtschaftsbereich trennen

Im selben Zug wurde Referat 5 neu ausgerichtet und zum Aufsichtsreferat über den gesamten Wirtschaftsbereich. Zugleich war es nötig, den Bereich der Sanktionen aus dem Wirtschaftsreferat herauszulösen, um hier die größtmögliche Unabhängigkeit zu gewährleisten. Verfahren zu Ordnungswidrigkeiten und Bußgeldern sollten daher künftig im neu gestalteten Referat 6 zentral bearbeitet werden.

## Themen der Zukunft im Blick

Ein immer wichtigeres Thema in allen Lebensbereichen ist die Digitalisierung. Die DS-GVO trägt dieser Entwicklung Rechnung, indem sie den Aufsichtsbehörden unter anderem aufgibt, „maßgebliche Entwicklungen (zu) verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie“. Um diese Pflicht erfüllen zu können und mit den innovativen Datensammlern aus der Wirtschaft auf Augenhöhe agieren zu können, habe ich ein Referat für sogenannte Zukunftsthemen eingerichtet.

Referat für Zukunftsthemen

Dort begleiten Kolleginnen und Kollegen sowohl mit hohem juristischen als auch technischen Sachverstand neue Entwicklungen und gestalten diese mit. Dazu gehören zum Beispiel das Internet der Dinge, Künstliche Intelligenz, Smart Data und Biometrie. Darüber hinaus befasst sich das Referat unter anderem auch mit Fragen des strategischen technisch-organisatorischen Datenschutzes, woraus bisher zum Beispiel der Prozess zur Auswahl angemessener Sicherungsmaßnahmen (ZAWAS) hervorgegangen ist.

Bericht zu ZAWAS siehe Seite 168

# 1.8 Die DS-GVO in der Praxis – so hat sich die Arbeit der Aufsicht verändert

Zum Ende des Berichtzeitraums hatte die Datenschutz-Grundverordnung (DS-GVO) gut sieben Monate Geltung. Mit der Verordnung haben sich aber nicht nur die Vorgaben für datenverarbeitende Stellen verändert, sondern auch die Arbeit der Aufsichtsbehörden, sowohl quantitativ als auch qualitativ.

Zunächst zum quantitativen Aspekt: Gerade in den Wochen vor und nach dem 25. Mai 2018 wurde meine Behörde förmlich von Beratungsanfragen überrollt. Gerade in den Bereichen Gesundheit, Vereine und Wirtschaft mussten meine Mitarbeiterinnen und Mitarbeiter ein Vielfaches des bisher Erfahrenen bewältigen.

Zahl der Eingänge verdoppelt

2017 erreichten meine Behörde insgesamt knapp 4700 Anfragen. Darin sind sämtliche Eingänge eingerechnet – Beschwerden, Anfragen, sonstige Eingaben – telefonisch, schriftlich und per E-Mail. 2018 waren es dagegen insgesamt knapp 10.000. Der Aufwand hatte sich also rein quantitativ innerhalb eines Jahres verdoppelt. Den größten Anteil daran hatten mit etwa 8300 Vorgängen die Beratungsanfragen.

## Einschränkung der individuellen Beratung

Hotline für Vereine

Ob dieses Andrangs musste ich kurzfristige Konsequenzen ziehen und die telefonische Erreichbarkeit sowie individuelle Beratungsleistungen deutlich einschränken. Eine Ausnahme ist hier bislang die Beratung von Vereinen und Verbänden. Für diese habe ich eigens eine telefonische Hotline eingerichtet, um gerade die ehrenamtlich Tätigen bestmöglich zu unterstützen. Ansonsten habe ich die Beratung weitgehend auf meine Webseite verlagert. Dort finden sich inzwischen eine Fülle an Handreichungen, Mustern und Frequently Asked Questions (FAQ) zu verschiedenen Themengebieten.

Zwar stellte dieser quantitative Anstieg schon eine große Belastung für meine Behörde dar. Noch weit bedeutender und herausfordernder waren und sind aber die qualitativen Veränderungen, welche die DS-GVO mit sich gebracht hat. Denn diese sieht für die Aufsichtsbehörden nicht nur umfangreiche Aufsichtsbefugnisse und weit reichende Sanktionsmöglichkeiten, sondern auch eine deutliche Ausweitung ihrer Aufgaben vor.

## Rechte von Beschwerdeführern gestärkt

Von großer Bedeutung ist zum Beispiel die Bearbeitung von Datenschutz-Beschwerden. Betroffene können sich formell bei meiner Behörde beschweren, wenn sie glauben, in ihren Datenschutz-Rechten verletzt worden zu sein. Zwar haben wir auch vor Geltung der DS-GVO solche Beschwerden geprüft, diese Arbeit hat aber nun eine ganz neue Qualität. Denn die DS-GVO stärkt die Rechte der Betroffenen deutlich. Sie verpflichtet die Aufsichtsbehörden dazu, jede Beschwerde angemessen zu prüfen und dem Beschwerdeführer innerhalb einer bestimmten Frist fundiert Auskunft über den Stand der Bearbeitung zu geben. Gelingt das nicht, kann der Betroffene Untätigkeitsklage einreichen. Diese Möglichkeiten gab es bislang nicht, weshalb ich jetzt noch höhere Ansprüche an die Bescheide stellen muss, die mein Haus verlassen. Allein 2018 erreichten mich mehr als 1000 Beschwerden nach DS-GVO.

Betroffener kann gegen die Aufsichtsbehörde klagen

## Meldepfiicht für Datenpannen verschärft

Ein weiterer großer Aufwandstreiber waren im Berichtszeitraum die Meldungen von Datenschutzverstößen nach Art. 33 DS-GVO, sogenannte Datenpannen. Für diese hat die DS-GVO die Meldepflicht deutlich verschärft. Deshalb war mir bereits vor Geltungsbeginn der Verordnung bewusst, dass ihre Zahl enorm zunehmen wird. Während mein Haus sich 2017 nur mit 20 Meldungen befassen musste, waren es 2018 rund 370. Da die DS-GVO zudem zur Prüfung einer Datenpanne den Begriff des Risikos ins Zentrum stellt, was vorher nicht so war, müssen meine Mitarbeiter auch hier mit völlig neuen Sachverhalten umgehen.

Zahl der gemeldeten Pannen steigt enorm

## Europäische Zusammenarbeit

Die vielleicht schwerste Aufgabe, die sich allen Aufsichtsbehörden in der EU schon stellt und in den kommenden Jahren weiter stellen wird, ist die europäische Zusammenarbeit. Kommt es zu grenzüberschreitenden Datenverarbeitungen, soll nun durch komplexe Mechanismen der Zusammenarbeit am Ende eine einheitliche Entscheidung der beteiligten Aufsichtsbehörden stehen. Unter Einhaltung kurzer Fristen müssen die Behörden Prozesse mit großem Abstimmungsbedarf abschließen.

Komplexe Mechanismen zur Abstimmung

Das hat auch Auswirkungen auf unsere Zusammenarbeit auf nationaler Ebene. Denn bevor sich die deutschen Aufsichtsbehörden in einem europäischen Verfahren äußern, müssen sie erst auf nationaler Ebene einen gemeinsamen Standpunkt erarbeitet haben. Auch das ist neu, nachdem meine Kollegen und ich Entscheidungen bislang völlig eigenständig treffen konnten.

Zur angemessenen Durchführung dieser europäischen Verfahren habe ich einen neuen Dienstposten eingerichtet. Dieser bearbeitete allein 2018 mehr als 500 Vorgänge, die über das Binnenmarktsystem IMI aus dem europäischen Raum aufgelaufen sind. Bei jedem dieser Vorgänge ist genau zu prüfen, ob meine Behörde betroffen ist. Dem entsprechend hat sich auch der Kontakt meines Hauses zu anderen europäischen Aufsichtsbehörden intensiviert.

Mehr zur europäischen Kooperation auf Seite 18

# D.2. JI-Richtlinie

## Neues Datenschutzrecht für Polizeibehörden

Neben der Datenschutz-Grundverordnung (DS-GVO) musste der Landesgesetzgeber auch die sogenannte JI-Richtlinie[1] in nationales Recht umsetzen. Diese enthält für Polizei- und Strafverfolgungsbehörden Regelungen, wenn es um Daten zur Strafverhütung oder -verfolgung geht. Bedauerlicherweise wurden die Vorgaben der Richtlinie unzureichend und unvollständig im Niedersächsischen Datenschutzgesetz umgesetzt. Der Gesetzgeber muss schnellstmöglich nachsteuern.

### Gesetzgebung im Schnelldurchgang

Zahlreiche Regelungslücken beim polizeilichen Datenschutz

Mit der JI-Richtlinie soll die Verarbeitung personenbezogener Daten bei Polizei und Strafverfolgungsbehörden annähernd auf einen einheitlichen Standard in der gesamten EU gebracht werden. Zudem werden die Betroffenenrechte der Bürgerinnen und Bürger gestärkt. Die Verarbeitung personenbezogener Daten durch die Polizei ist für die betroffenen Bürgerinnen und Bürger besonders sensibel. Umso bedauerlicher ist es, dass das Niedersächsische Innenministerium die zweijährige Übergangsfrist der JI-Richtlinie nicht genutzt hat, um einen diskussionsfähigen Gesetzentwurf zu erarbeiten.

Wenig Zeit für inhaltliche Prüfung

Erst Anfang April 2018 legten die Regierungsfraktionen einen Gesetzentwurf für die Paragrafen 23 bis 58 des Niedersächsischen Datenschutzgesetzes (NDSG) vor. Für eine inhaltlich fundierte Prüfung bis zur Anhörung im Innenausschuss am 27.4.2018 blieb nur wenig Zeit. Dennoch unterbreitete meine Behörde den Abgeordneten mehr als 40 Änderungsvorschläge, die jedoch wegen der Verabschiedung des Gesetzes im Mai nahezu unberücksichtigt blieben. Beispiele dieser Vorschläge sind:

- Zukünftig muss die Polizei bei der Datenverarbeitung zwischen verschiedenen Kategorien betroffener Personen unterscheiden, so z. B. zwischen Täter-, Opfer- oder Zeugendaten. Diese Maßgabe setzt Niedersachsen bisher nicht ausreichend um.

1 Richtlinie Nr. 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016

- Dies betrifft auch die Vorgabe, dass die Polizei zukünftig die Daten danach zu kategorisieren hat, ob diese auf Fakten oder auf einer persönlichen Einschätzung beruhen.
- Ferner entsprechen die Regelungen zur nachträglichen Information der Betroffenen, wenn Daten ohne deren Wissen durch die Polizei verarbeitet werden, nicht den europarechtlichen Vorgaben.
- Auch werden der Landesbeauftragten nur unzureichende Abhilfebefugnisse eingeräumt, wenn die polizeiliche Datenverarbeitung gegen geltendes Recht verstößt. So können in diesen Fällen keine vollstreckbaren Anordnungen getroffen werden, sondern es bleibt bei dem Instrument der folgenlosen Beanstandung oder Warnung.

## Verschlechterung des Datenschutzes

Aufsicht über Polizei und Justiz erheblich eingeschränkt

Der im Mai 2018 verabschiedete 2. Teil des NDSG zur Umsetzung der JI-Richtlinie ist nicht nur unvollständig und damit an zahlreichen Stellen europarechtswidrig. Die Regelungen der §§ 23 bis 58 NDSG verschlechtern den Datenschutz auch im Vergleich zu den alten Regelungen an mehreren Stellen erheblich. So ist eine datenschutzrechtliche Aufsicht über die Datenverarbeitung bei Strafverfolgungsbehörden zukünftig erst dann möglich, wenn das strafrechtliche Ermittlungsverfahren abgeschlossen ist. Auch die Strafvollstreckung ist einer datenschutzrechtlichen Kontrolle bis zum Abschluss des Verfahrens entzogen. Damit wird die Aufsicht meiner Behörde im Bereich der Polizei- und Justizbehörden erheblich eingeschränkt. Meiner Ansicht nach verstößt dies gegen europäisches Recht.

§ 40 Abs. 5 NDSG widerspricht dem Grundsatz des „Privacy by Design“

Ferner darf die Polizei zukünftig anders als bisher Datenverarbeitungssysteme in Betrieb nehmen, ohne zuvor von meiner Behörde geäußerte Bedenken und Empfehlungen zu berücksichtigen. Die beabsichtigte Datenverarbeitung muss für die Aufgabenerfüllung nur erhebliche Bedeutung besitzen und besonders dringlich sein. Zwar sind dann die Bedenken und Empfehlungen nachträglich von der Polizeibehörde zu berücksichtigen. Die Vergangenheit hat jedoch gezeigt, dass mit der Inbetriebnahme von Datenverarbeitungssystemen diese nachträglich nur noch schwer datenschutzrechtlich angepasst werden können. Auch sind damit in der Regel erhebliche Mehrkosten verbunden. Schließlich widerspricht diese Vorgehensweise dem datenschutzrechtlichen Grundsatz „Privacy by Design“. Dieser besagt, dass Datenschutzaspekte bereits bei der Technikgestaltung geregelt sein sollten, bevor die verantwortliche Stelle mit der Datenverarbeitung beginnt.

# D.3. E-Privacy-Verordnung

## Warten auf die E-Privacy-Verordnung

Die mit der Datenschutz-Grundverordnung (DS-GVO) eingeläutete europäische Datenschutzreform soll für den Bereich der elektronischen Kommunikation durch die E-Privacy-Verordnung weitergeführt werden. Ursprünglich war geplant, dass beide Verordnungen zeitgleich am 25. Mai 2018 in Kraft treten. Während die DS-GVO aber schon vor ihrer ersten Evaluierung steht, ist die Zukunft der E-Privacy-Verordnung immer noch ungewiss.

Die E-Privacy-Verordnung (E-Privacy-VO) soll die E-Privacy-Richtlinie (E-Privacy-RL) aus dem Jahr 2002 (zuletzt geändert durch die sogenannte Cookie-Richtlinie im Jahr 2009) ersetzen. Es entstand zunächst der Eindruck, dass dieses ambitionierte Vorhaben gelingen könnte. Die EU-Kommission hatte im Januar 2017 ihren Vorschlag einer E-Privacy-VO in das Gesetzgebungsverfahren eingebracht.

Informationen zur E-Privacy-VO -Kurzlink: https://t1p.de/EPrivacyVO

Das Europäische Parlament arbeitete zügig weiter. Im Sommer 2017 folgten Stellungnahmen durch die Art. 29-Datenschutzgruppe sowie vier Ausschüsse des EU-Parlaments (ITRE-, IMCO-, JURI- und LIBE-Ausschuss). Seit Oktober 2017 liegt der Entwurf einer legislativen Entschließung des Europäischen Parlaments vor.

### Bisher kein Entwurf des Europäischen Rates

Doch der Europäische Rat lässt sich Zeit – viel Zeit – für die Beratung und hat bis Januar 2019 keinen Entwurf in das Verfahren eingebracht. Es ist somit nicht absehbar, wann die Verhandlungen zwischen den beteiligten Gesetzgebungsorganen EU-Rat, EU-Parlament und EU-Kommission beginnen werden. Sicher ist allerdings, dass es einen hohen Diskussionsbedarf gibt, da bereits der Entwurf des EU-Parlaments wesentliche Änderungsvorschläge gegenüber dem Erstentwurf der EU-Kommission enthält.

Hoher Diskussionsbedarf absehbar

Ein weiterer Unsicherheitsfaktor sind die im Mai 2019 anstehenden Europawahlen. Das Gesetzgebungsverfahren zur E-Privacy-VO müsste bei der Neuwahl des Parlaments zwar nicht zwingend neu aufgerollt werden, allerdings obliegt die Entscheidung darüber den zuständigen Organen der EU. Sollte es zum Erlass der E-Privacy-VO kommen, wird es zudem eine Übergangsfrist geben, die zwischen einem und zwei Jahren liegen wird.

Neues Verfahren nach der Wahl?

## Was ändert sich durch die E-Privacy-Verordnung?

Die E-Privacy-VO dient dem Schutz der Vertraulichkeit und personenbezogener Daten bei der elektronischen Kommunikation – insbesondere über das Internet. Die wichtigsten Änderungen:

### 1. Verordnung statt Richtlinie

Einheitliches Schutzniveau in Europa

Die erste wesentliche Änderung ist der Wechsel des Regelungsinstruments für den Bereich der elektronischen Kommunikation – von einer Richtlinie zu einer Verordnung. Ziel einer Verordnung ist es, ein europaweites Schutzniveau und einen einheitlichen Rechtsrahmen für Unternehmen zu erreichen. Die E-Privacy-VO wird ebenso wie die DS-GVO in Deutschland unmittelbar anwendbares Recht sein.

### 2. Erweiterung des Anwendungsbereichs

Anwendung auch auf moderne Dienste

Die geplante E-Privacy-VO soll im Unterschied zur E-Privacy-RL nicht nur auf klassische Telekommunikationsdienste, wie Telefon, E-Mail oder SMS/MMS, anwendbar sein. Stattdessen soll sie auch für moderne Kommunikationsdienste gelten wie Bildtelefon, Messenger und Social Networks, wie sie z.B. durch WhatsApp, Skype, Viber oder iMessage angeboten werden. Diese Dienstangebote werden unter der Bezeichnung Over-the-Top-Kommunikationsdienste (OTT-Dienste) in die E-Privacy-VO aufgenommen.

### 3. Einheitliches Schutzniveau für Kommunikationsinhalte und -metadaten

Der sachliche Anwendungsbereich der Verordnung soll die Verarbeitung elektronischer Kommunikationsdaten, die einen Bezug zum Nutzer ermöglichen, betreffen. Dies umfasst elektronische Kommunikationsinhalte und elektronische Kommunikationsmetadaten. Es handelt sich dabei z. B. um Daten, die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts eines Kommunikationsvorgangs, des geografischen Standorts sowie von Datum, Uhrzeit, Dauer und Art der Kommunikation verwendet werden.

Daten unterliegen dem Fernmeldegeheimnis

Diese Kommunikationsdaten unterliegen dem Fernmeldegeheimnis und sollen vertraulich behandelt werden müssen. Ausnahmen vom Vertraulichkeitsschutz sind nur in sehr engen Grenzen zulässig und müssen ausdrücklich von der Verordnung vorgesehen werden. Die Erfassung und Verarbeitung elektronischer Kommunikationsdaten soll grundsätzlich auf das funktional Notwendige begrenzt werden. Für andere Zwecke soll die Nutzung der Daten nur erlaubt sein, wenn sie anonymisiert sind oder der Nutzer ausdrücklich eingewilligt hat.

### 4. Neue Regelung zur Verfolgung des Nutzers (Tracking)

Der Kommissionentwurf der Verordnung sieht die grundsätzliche Differenzierung zwischen der Erfassung des Nutzerverhaltens im Internet, dem sogenannten Online-Tracking, und dem Offline-Tracking vor. Das Online-Tracking wurde ursprünglich vor allem durch den Einsatz von Cookies umgesetzt. Seit einiger Zeit kommen aber auch andere technische Verfahren, wie z. B. Browser-Fingerprints zum Einsatz. Dieses Tracking verlangt nach der E-Privacy-RL für die datenschutzkonforme Umsetzung die vorherige ausdrückliche Einwilligung des Nutzers.

Durch Offline-Tracking werden die Bewegungen des Nutzers im realen Raum, z. B. in der Innenstadt oder in Verkaufsräumen erfasst. Spezielle Regelungen existieren hierfür bislang nicht.

Online-Tracking soll untersagt werden

Die E-Privacy-VO will das Online-Tracking untersagen, es sei denn, es erfolgt mittels anonymer Daten oder der Nutzer hat eingewilligt. Die hierfür erforderliche Erhebung von Informationen aus den genutzten Geräten soll abgesehen von abschließend geregelten Ausnahmefällen nur mit Einwilligung des Nutzers erlaubt sein.

Der Entwurf der europäischen Kommission sieht vor, dass das Offline-Tracking schon dann erlaubt sein soll, wenn es einen deutlichen Hinweis auf den Einsatz dieses Verfahrens gibt und der Nutzer darüber informiert wird, was er tun kann, um die Erhebung zu beenden oder auf ein Minimum zu beschränken.

### 5. Pflichten für Anbieter von Software

Die E-Privacy-VO sieht erstmals vor, die Anbieter von Software zu Datenschutzmaßnahmen zu verpflichten (Privacy by Design). Erstens soll jede Software, die eine elektronische Kommunikation erlaubt (wie Internetbrowser) die technische Möglichkeit bieten zu verhindern, dass Dritte Informationen in den genutzten Geräten und Browsern speichern oder bereits gespeicherte Informationen verarbeiten.

Zweitens ist vorgesehen, dass der Nutzer bei der Installation von Software über mögliche Einstellungen zur Privatsphäre informiert werden und zur Fortsetzung der Installation seine Einwilligung zu einer Einstellung geben muss.

### 6. Erhöhung von Bußgeldern

In Übereinstimmung mit der DS-GVO soll der Bußgeldrahmen wesentlich ausgeweitet werden. Für einzelne Verstöße gegen die Vorschriften der E-Privacy-VO sind Geldbußen von bis zu 20 Millionen Euro oder von bis zu 4 Prozent des weltweiten Konzernumsatzes des vergangenen Geschäftsjahres vorgesehen.

Geldbußen bis 20 Mio. Euro

## Rechtliches Vakuum

Solange die E-Privacy-VO nicht in Kraft ist, besteht für den Datenschutz bei der elektronischen Kommunikation ein rechtliches Vakuum, das nur notdürftig durch die Anwendung der DS-GVO geschlossen werden kann.

Mit Anwendbarkeit der DS-GVO können weder die Datenschutzvorschriften des Telemediengesetzes (TMG) noch die der E-Privacy-RL beibehalten werden. Darauf hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits im April 2018 durch die Positionsbestimmung zur Anwendbarkeit der Vorschriften des Telemediengesetzes aufmerksam gemacht. Es fehlt daher seit dem 25. Mai 2018 an risikoadäquaten Vorgaben für diesen in der Praxis so wichtigen Anwendungsbereich. Ich sehe es daher als dringend notwendig an, dass die E-Privacy-Verordnung so schnell wie möglich erlassen wird.

Zur Positionsbestimmung der DSK siehe Seite 162

# E. Datenschutzkonferenz

## E.1. Politik und Wirtschaft im Fokus:

## Niedersachsens Vorsitz in der Datenschutzkonferenz

Am 24. Januar 2017 übernahm Niedersachsen den Vorsitz in der Konferenz der unabhängigen deutschen Datenschutzbehörden (DSK) von Mecklenburg-Vorpommern. Bereits ein Jahr vor Geltung der Datenschutz-Grundverordnung bestimmte das neue europäische Recht die Agenda der DSK maßgeblich – und damit auch das niedersächsische Vorsitzjahr. Jenseits der Klärung rechtlicher Fragen und der Vereinbarung gemeinsamer Standpunkte richtete die Konferenz ihr Augenmerk darauf, die kommenden Anforderungen und Erwartungen der Aufsichtsbehörden gegenüber Politik und Wirtschaft zu artikulieren.

Während meines Vorsitzes berieten sich die Aufsichtsbehörden in zwei Hauptkonferenzen und fünf Sondersitzungen zu einem gemeinsamen Verständnis und einer einheitlichen Auslegung der Datenschutz-Grundverordnung (DS-GVO).

**Die Datenschutzkonferenz (DSK)**
Die Datenschutzkonferenz besteht aus den unabhängigen Datenschutzbehörden des Bundes und der Länder. Seit 1978 widmet sich die Konferenz der Aufgabe, die Datenschutzgrundrechte zu wahren und zu schützen, eine einheitliche Anwendung des europäischen und nationalen Datenschutzrechts zu erreichen sowie gemeinsam für seine Fortentwicklung einzutreten. Hierzu veröffentlicht die DSK Entschließungen, Beschlüsse, Orientierungshilfen, Standardisierungen, Stellungnahmen, Pressemitteilungen und Festlegungen. Die regelmäßigen Sitzungen dienen der Meinungsbildung zu Fragen und Themen, denen aus Sicht des Datenschutzes eine besondere Bedeutung zukommt. Der Vorsitz wechselt jährlich unter den Aufsichtsbehörden.

Appell an den Bundestag

Vor der Bundestagswahl 2017 wandte sich die DSK erstmals seit ihrem Bestehen mit einem politischen Appell direkt an die Fraktionen. Dabei formulierte sie elf handlungsorientierte Grundforderungen an die Mitglieder des neuen Bundestages.

## Künftige Abgeordnete für Datenschutz gewinnen

Ziel der Forderungen war es, das Datenschutzrecht weiter zu entwickeln sowie dessen Durchsetzung und Akzeptanz zu fördern. Mit der Bundestagswahl bot sich die Gelegenheit, um die aktuellen und künftigen Abgeordneten für die Belange des Datenschutzes zu sensibilisieren. Gleichzeitig war es der passende Moment kurz vor dem Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO), die Positionen und Erwartungen der deutschen Datenschützer deutlich zu machen.

Forderungen der DSK – Kurzlink: https://t1p.de/Forderungen-Bundestag

In einer Sondersitzung stimmten die Datenschutzbeauftragten des Bundes und der Länder ihre Forderungen an den künftigen Bundestag ab. Die erfolgreiche Zusammenarbeit an diesem gemeinsamen Appell zeigt, wie gut die föderale Struktur des Datenschutzes trotz Unabhängigkeit der einzelnen Behörden funktionieren kann. Dies ist umso wichtiger, da es unter der DS-GVO besonders darauf ankommt, dass die deutschen Aufsichtsbehörden kurzfristig gemeinsame Standpunkte finden, um eine gemeinsame deutsche Position auf europäischer Ebene einzubringen.

## Dialog mit der Wirtschaft

Neue Zusammenarbeit zwischen Aufsicht und Wirtschaft

Bereits mit Inkrafttreten der DS-GVO war absehbar, dass sich durch die neuen Strukturen, Regularien und Zuständigkeiten im europäischen Datenschutzrecht neue Formen des Zusammenwirkens von Aufsichtsbehörden auf der einen Seite und den Wirtschaftsunternehmen auf der anderen Seite ergeben würden. Und zwar nicht allein bei Vollzugsfragen, sondern in besonderem Maße im Bereich der Prävention, der durch die DS-GVO deutlich gestärkt wird.

Unter diesen Vorzeichen war es naheliegend, dass die DSK in einen direkten Austausch mit der Wirtschaft trat. Im Rahmen einer Sonderkonferenz im Juni 2017 kam es in Hannover zu einem ersten Austausch. Dabei ging es nicht darum, Wirtschaftsvertretern Zugeständnisse, etwa im Bereich der Sanktions-

maßnahmen zu unterbreiten oder Erleichterungen bei der Umsetzung der DS-GVO einzuräumen. Vielmehr war es das Ziel, die Erwartungen der jeweils anderen Seite kennenzulernen und künftig besser einschätzen zu können.

Dialog macht Unterschiede deutlich

Wenig überraschend fiel das Urteil über die Anforderungen der DS-GVO und die Lesart teilweise durchaus unterschiedlich aus. Dennoch bekräftigten sowohl die Datenschutzbeauftragten als auch die Wirtschaftsvertreter den Nutzen des Treffens, weil im offenen Dialog die unterschiedlichen Herangehensweisen und Verständnisse der Grundverordnung deutlich wurden.

## Datenschutztag im Zeichen der Digitalisierung

Der Europäische Datenschutztag ist der traditionelle Ausklang eines Vorsitzjahres in der DSK und offizielles Übergabedatum an den folgenden Vorsitzführer, in diesem Fall Nordrhein-Westfalen. Unter dem Vorsitz Niedersachsens lautete die Leitfrage des 12. Europäischen Datenschutztages „Souveränität in der digitalen Welt – eine Illusion?“. Mit dieser Themenwahl wurde auch ein Bogen gezogen, zu der DSK-Entschließung „Göttinger Erklärung: Vom Wert des Datenschutzes in der digitalen Gesellschaft“ die in der 93. Sitzung im März 2017 verabschiedet wurde. Maßgeblich für diese Leitfrage war der immer wieder vorgebrachte Vorwurf von Politik, Wirtschaft und Verbänden, dass Datensparsamkeit, Datenvermeidung und Zweckbindung Eckpfeiler eines überholten Verständnisses von Datenschutz seien.

Souveränität in der digitalen Welt

Die Leitfrage war bewusst provokant formuliert und entsprechend kontrovers diskutierten die geladenen Digitalisierungsexperten vor rund 160 Teilnehmern im Forum der niedersächsischen Landesvertretung in Berlin, wie Digitale Souveränität auf der Basis bestehender Datenschutz-Grundsätze entstehen kann.

# E.2. Datenschutzkonferenz

## Veröffentlichungen der Datenschutzkonferenz unter niedersächsischem Vorsitz

Die Vorbereitung der Aufsichtsbehörden auf die Datenschutz-Grundverordnung (DS-GVO) hat den niedersächsischen Vorsitz in der Datenschutzkonferenz geprägt. Eine besondere Herausforderung, denn gleichzeitig erforderten auch tagesaktuelle Themen das entschlossene Auftreten der Datenschützer.

Der Geltungsbeginn der DS-GVO im Mai 2018 war bereits 2017, in Niedersachsens Vorsitzjahr in der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), das bestimmende Thema. Dennoch kreisten die Beratungen des Datenschutzbeauftragten nicht ausschließlich um die DS-GVO. Themen wie die Auswirkungen der Digitalisierung, der Umgang mit biometrischen Daten oder der Dauerbrenner Vorratsdatenspeicherung erforderten regelmäßig, zum Teil auch kurzfristige, Stellungnahmen.

### Entschließungen der Datenschutzkonferenz

Den grundsätzlichen Wert des Datenschutzes für die Belange und Rechte der Bürger in einer durch die Digitalisierung geprägten Gesellschaft betonte die DSK mit ihrer „Göttinger Erklärung". Datenschutz, so die Botschaft der Erklärung, ist kein Hindernis für die gesellschaftliche und wirtschaftliche Entwicklung, sondern Garant der informationellen Selbstbestimmung und eine wesentliche Voraussetzung für das Gelingen der Digitalisierung unter individuell-freiheitlichen Vorzeichen.

In weiteren Entschließungen positionierte sich die DSK unter anderem zu Fragen der Speicherung von und dem Bundeskriminalamtgesetz. Ausschlaggebend für eine schriftliche Intervention der Datenschutzaufsichtsbehörden war dabei jeweils der Schutz personenbezogener Daten vor einem überzogenen und nicht notwendigen Zugriffsanspruch durch den Gesetzgeber.

Entschließungen der DSK – Kurzlink: https://t1p.de/DSK-Entschliessungen

**Entschließungen während des niedersächsischen DSK-Vorsitzes im Überblick:**

**94. Konferenz am 08./09.11.2017 in Oldenburg**

- Entschließung „Keine anlasslose Vorratsspeicherung von Reisedaten“
- Entschließung Umsetzung der DSGVO im Medienrecht

**93. Konferenz am 29./30.03.2017 in Göttingen**

- Entschließung „Göttinger Erklärung:
  Vom Wert des Datenschutzes in der digitalen Gesellschaft“
- Entschließung „Einsatz von Videokameras zur biometrischen
  Gesichtserkennung birgt erhebliche Risiken“

**Entschließungen zwischen den Konferenzen**

- Entschließung „Einsatz externer Dienstleister durch Berufsgeheimnisträger
  rechtssicher und datenschutzkonform gestalten!“
- Entschließung „Neues Bundeskriminalamtgesetz - Informationspool
  beschneidet Grundrechte“
- Entschließung „Gesetzesentwurf zur Aufzeichnung von Fahrdaten ist völlig
  unzureichend!“

**Sonderkonferenz am 24.01.2017 in Hannover**

- Entschließung „Novellierung des Personalausweisgesetzes – Änderungen
  müssen bürger- und datenschutzfreundlich realisiert werden!“

## Bundesratsinitiative zum BDSG

Mit der bevorstehenden Geltung der DS-GVO hatten standen die EU-Staaten vor der Aufgabe, ihr jeweiliges nationales Datenschutzrecht an die europäische Verordnung anzupassen und, wenn gewollt, um weiterreichende Regelungen zu ergänzen. Den Anpassungsprozess des Bundesdatenschutzgesetzes (BDSG) verfolgten die deutschen Aufsichtsbehörden entsprechend aufmerksam und kritisch. Bereits der erste Entwurf enthielt zahlreiche Mängel, sodass die Datenschutzbeauftragten des Bundes und der Länder umfassenden Handlungsbedarf sahen.

Unter Federführung meiner Behörde wurde ein Redaktionsteam gebildet, um die Änderungsanträge der einzelnen Aufsichtsbehörden zu bündeln und fristgerecht an den Bundesrat zu übermitteln. Erfreulich ist die Tatsache, dass die behördenübergreifende Zusammenarbeit besonders reibungslos funktionierte. Leider wurden letztlich durch den Bundesrat nur einige Forderungen der DSK im Gesetzgebungsverfahren aufgegriffen.

## Kurzpapiere zur DS-GVO

Den Verantwortlichen in der Wirtschaft stellte die DSK bereits vor Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) mit zahlreichen Kurzpapieren praxisorientierte Handlungsempfehlungen zur Verfügung. Sie dienen als erste Orientierungshilfe, wie die DS-GVO im praktischen Vollzug angewendet werden sollte. Diese Initiative wurde von den Unternehmen sehr wohlwollend aufgenommen und dürfte wesentlich dazu beigetragen haben, die anfänglich häufig wahrzunehmende Verunsicherung im Wirtschaftsbereich ein Stück weit aufzulösen.

Ausführlicher Bericht zum BDSG ab Seite 26

Mehr zu den Kurzpapieren ab Seite 23

# F. Aktuelle Themen

## F.1. Herausragende Rechtsprechung auf europäischer und Bundesebene

### 1.1 Europäischer Gerichtshof nimmt Fanpage-Betreiber in die Pfiicht

Am 15. Juni 2018 hat der Europäische Gerichtshof (EuGH) entschieden, dass die Betreiber einer sogenannten Fanpage im sozialen Netzwerk Facebook neben dem amerikanischen Unternehmen selbst ebenfalls im datenschutzrechtlichen Sinne als „Verantwortliche“ zu werten sind. Diese Entscheidung bricht eine Lanze für die Tätigkeit der Aufsichtsbehörden und stärkt den Datenschutz in Europa.

Die Entscheidung des EuGH geht zurück auf eine Anordnung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) gegen die Wirtschaftsakademie Schleswig-Holstein GmbH, ein privatrechtlich organisiertes Bildungsunternehmen. Im November 2011 ordnete das ULD gegenüber der Wirtschaftsakademie an, ihre bei Facebook betriebene Fanpage zu deaktivieren. Begründet wurde dies damit, dass weder die Wirtschaftsakademie noch Facebook die Besucher der Fanpage darauf hinwiesen, dass Facebook mittels Cookies von ihnen personenbezogene Daten erhebe und diese Daten danach verarbeitet.

Frage: Wer ist für die Verarbeitung verantwortlich?

Nachdem der Widerspruch der Wirtschaftsakademie gegen diesen Bescheid erfolglos geblieben war, begann der Weg durch die Gerichtsinstanzen. Kern der gerichtlichen Auseinandersetzung war vor allem die Frage, ob die Wirtschaftsakademie für Datenverarbeitungen verantwortlich gemacht werden kann, die faktisch allein vom Netzwerkbetreiber Facebook vorgenommen werden. Das Bundesverwaltungsgericht (BVerwG) legte unter anderem diese Frage dem EuGH zur Vorabentscheidung vor.

## Kernaussagen der EuGH-Entscheidung

Gericht stellt gemeinsame Verantwortung fest

Der EuGH hat in aller Deutlichkeit festgestellt, dass der Betreiber einer bei einem sozialen Netzwerk unterhaltenen Fanpage datenschutzrechtlich verantwortlich ist. Damit wurde die auch von mir bereits in der Vergangenheit vertretene Rechtsauffassung höchstrichterlich bestätigt. Dem steht nicht entgegen, dass auch Facebook selbst datenschutzrechtlich verantwortlich ist. Der EuGH betont, dass für Datenverarbeitungen im Zusammenhang mit dem Betrieb einer Fanpage der Betreiber der Seite und Facebook gemeinsam verantwortlich sind.

Entschließungen der DSK - Kurzlink: https://www.datenschutzkonferenz-online.de/entschliessungen.html

Für alle öffentlichen und nicht-öffentlichen Betreiber von Fanpages in Deutschland bedeutet diese Entscheidung, dass die „Zeit der Verantwortungslosigkeit“ nun vorbei ist. So formuliert es Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in ihrer Entschließung vom 6. Juni 2018 zur EuGH-Entscheidung hervor. Die Seitenbetreiber können nicht mehr auf die ausschließliche datenschutzrechtliche Verantwortlichkeit von Facebook verweisen, sondern sind selbst mitverantwortlich für die Einhaltung des Datenschutzes gegenüber den Besuchern ihrer Fanpage. Sie müssen sich bereits fragen, ob der Betrieb einer Fanpage grundsätzlich mit dem Datenschutzrecht vereinbar ist. Welche konkreten Einzelfragen hierbei zu berücksichtigen sind, hat die DSK in einem weiteren Beschluss zu Facebook-Fanpages am 5. September 2018 als Hilfestellung für die Betreiber veröffentlicht.

## Konsequenzen für Facebook

Facebook muss Informationen bereit stellen

Auch für das amerikanische Unternehmen Facebook Inc. hat die Entscheidung des EuGH weitreichende Folgen. Aufgrund der gemeinsamen Verantwortlichkeit ist auch Facebook zum Handeln verpflichtet, sofern zukünftig ein datenschutzkonformer Betrieb von Fanpages ermöglicht werden soll.

Facebook muss erstens mit jedem Betreiber einer Fanpage einen die Vorgaben der DS-GVO einhaltenden Vertrag über die gemeinsame Verantwortlichkeit abschließen. Zweitens muss Facebook aber vor allem, den Betreibern von Fanpages umfassende Informationen darüber zu Verfügung stellen, in welcher Art und Weise die durch den Besuch der Fanpages erhobenen Nutzerdaten für die unterschiedlichen Geschäftszwecke verarbeitet werden. Letztlich muss Facebook seine Datenverarbeitungen transparent machen – für Betreiber und Nutzer der Fanpage und auch für die Aufsichtsbehörden. Eine Pflicht, der Facebook in der Vergangenheit nicht nachgekommen ist.

## Appell an die Landesverwaltung

In der niedersächsischen Landesverwaltung werden von zahlreichen Stellen Fanpages betrieben. Meine Bemühungen in den vergangenen Jahren, dass die Fanpages von den zuständigen öffentlichen Stellen gelöscht werden, waren bislang gescheitert. Die Entscheidung des EuGH habe ich zum Anlass genommen, die niedersächsischen Ministerien, die Fanpages betreiben, über das Urteil zu informieren und auf die gemeinsame Verantwortlichkeit hinzuweisen. Da auf dieser Grundlage bisher ein datenschutzkonformer Betrieb einer Fanpage nicht möglich ist, habe ich die Stellen nachdrücklich aufgefordert, die Seiten zu deaktivieren. Die Ministerien sind dieser Aufforderung jedoch im Berichtszeitraum nicht nachgekommen.

Datenschutzkonformer Betrieb nicht möglich

# 1.2 Fluggastdaten – Reisende unter Verdacht

Seit Jahren besteht Uneinigkeit zwischen Sicherheitsbehörden und Datenschützern über die Nutzung von personenbezogenen Daten Flugreisender zur Terrorabwehr und Strafverfolgung. Im Jahr 2017 legte der Europäische Gerichtshof in einem Gutachten wichtige Maßstäbe für diese Nutzung von Fluggastdaten fest und stützte damit den Datenschutz.

## Neue Entwicklungen in einem alten Streit

Fluggastdaten (Passenger Name Records – PNR) werden bei Buchung eines Fluges von den Fluggesellschaften erfasst und gespeichert: Name, Anschrift, Telefonnummer, Kreditkarteninformationen, Reiseverlauf, Reisepartner, Ernährungsgewohnheiten, allgemeine Bemerkungen zu den reisenden Personen etc. Es handelt sich teilweise um durchaus sensible Informationen, die auch von Interesse für die Sicherheits- und Strafverfolgungsbehörden sind.

Erfassung zahlreicher Daten bei der Buchung

Täter im Bereich des internationalen Terrorismus und der schweren Kriminalität agieren häufig grenzüberschreitend und reisen in andere Staaten. Seit Jahren wird daher darüber diskutiert, wie diese Daten für die Sicherheit der Einreiseländer und für die Strafverfolgung genutzt werden können und wie gleichzeitig der Datenschutz aller betroffenen Reisenden gewährleistet werden kann. Die EU schloss in den vergangenen Jahren mehrere Abkommen mit Staaten wie den USA und Australien, um eine Rechtsgrundlage für die Übermittlung der Daten Reisender zu schaffen. Der Europäische Gerichtshof (EuGH) brachte sich hat sich 2017 mit einem fachlichen Gutachten wegweisend in die Diskussion ein.

Im Jahr 2014 nutzte das EU-Parlament die Möglichkeit, ein Gutachten des EuGH zur Vereinbarkeit einer geplanten weiteren Übereinkunft zur Nutzung von Fluggastdaten mit den EU-Verträgen einzuholen. Die EU-Kommission hatte nämlich den Entwurf eines Abkommens mit Kanada über die Erhebung und Speicherung von Fluggastdaten vorgelegt. Das Parlament hatte Zweifel an der Vereinbarkeit des Abkommens mit den EU-Datenschutzrechten.

Parlament lässt Abkommen mit Kanada prüfen

## Richtlinie zu Fluggastdaten verabschiedet

In der Zwischenzeit verabschiedete die EU auch die Richtlinie über die Verwendung von Fluggastdatensätzen zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Diese ermöglicht den EU-weiten Austausch von Fluggastdaten zwischen den zuständigen Behörden. Die Daten sollen für einen Zeitraum von fünf Jahren vorgehalten werden, wobei sie nach dem Ablauf von sechs Monaten unkenntlich zu machen sind. Die Richtlinie wurde am 27.4.2017 mit dem Fluggastdatengesetz in deutsches Recht umgesetzt, welches zudem die Speicherung auf innereuropäische und deutsche Flüge ausweitet.

Daten werden 5 Jahre gespeichert

Folglich wird jede mit der Flugbuchung erlangte Information zu größtenteils unverdächtigen Personen ohne besonderen Anlass und ohne eine Verhältnismäßigkeitsprüfung pauschal für fünf Jahre gespeichert. Hierin lässt sich ohne weiteres eine unzulässige Vorratsdatenspeicherung erkennen. In der Zusammenschau lassen sich zudem aus Fluggastdaten Reisegewohnheiten, Beziehungen zwischen mehreren Personen sowie Informationen über die finanzielle Situation der Fluggäste ziehen. Sogar Gesundheitsdaten können offenbart werden. Durch die Erhebung und Verwendung von Fluggastdaten wird folglich in erheblicher Weise in das Privatleben Reisender eingegriffen.

Erhebliche Eingriffe in die Privatsphäre

## Abkommen mit Kanada kommt nicht zustande

Im Juli 2017 endlich äußerte sich der EuGH zum geplanten Fluggastdaten-Abkommen mit Kanada und leistete damit einen wichtigen Beitrag zur Diskussion. Der EuGH stellte fest, dass das Abkommen mit dem vorliegenden Inhalt nicht geschlossen werden darf, weil mehrere seiner Bestimmungen gegen die EU-Grundrechte verstoßen, insbesondere gegen das Grundrecht auf Achtung des Privatlebens und das Grundrecht auf Schutz personenbezogener Daten.

Im Einzelnen führte der EuGH aus, dass die Übermittlung von besonders sensiblen Daten wie Gesundheitsdaten, Informationen über politische Meinungen, religiöse Überzeugungen oder die ethnische Herkunft einer besonders fundierten und präzisen Rechtfertigung bedürfen – der pauschal formulierte Schutz vor Terrorismus und schwerer Kriminalität allein genügt nicht. Weiter ist es nicht akzeptabel, wenn die Daten der Reisenden nach der Einreise in Kanada ohne weitere Erkenntnisse bzw. ohne ein weiteres konkretes Verfahren von den kanadischen Behörden verwendet werden, da der entsprechenden Personen schließlich einmal die Einreise gestattet wurde. Nur bei Vorliegen eines konkreten Verdachts gegen eine Person ist die Speicherung ihrer Reisedaten weiterhin zulässig.

Fehlende Informationsrechte und Kontrolle

Weitere Bestimmungen des Abkommens waren nach Auffassung des EuGH zu unklar oder es fehlten genau geregelte Schutzmaßnahmen. Bemängelt wurden außerdem das Fehlen eines Informationsrechts der betroffenen Personen und einer unabhängigen Kontrollstelle.
Da das EuGH-Gutachten bindend ist, konnte das Abkommen nicht geschlossen werden.

## Der EuGH setzt Maßstäbe

Allgemein gültige Kriterien zu Fluggastdaten

Auch wenn sich dieses Gutachten auf das geplante Abkommen mit Kanada bezog, setzte der EuGH hier klare Maßstäbe für jede Verwendung von Fluggastdaten. Der EuGH stellte allgemeine Kriterien für Regelungen über Fluggastdaten auf:

- Beachtung des Grundrechts auf Datenschutz
- Besondere Anforderungen an die Rechtfertigung eines Grundrechtseingriffs
- Besonderer Schutz von sensiblen Daten
- Einrichtung einer unabhängigen Kontrollstelle
- Gewährung von Betroffenenrechten
- Begrenzung der Speicherdauer auf das unbedingt Erforderliche

## Datenschützer fordern: Nationales Recht anpassen

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) stellte in ihrer Entschließung vom 9.11.2017 klar, dass aus ihrer Sicht der vom EuGH vorgegebene Maßstab auf alle Fluggastdaten-Instrumente übertragbar sei. Der EuGH mache grundlegende Aussagen zur Speicherung und Übermittlung von Fluggastdaten.

Die Regelungen der bestehenden anderen Abkommen der EU und auch der Fluggastdaten-Richtlinie seien identisch oder vergleichbar mit den im Kanada-Abkommen kritisierten Bestimmungen. Als Folge forderte die DSK, sämtliche Fluggastdaten-Instrumente der EU und auch das deutsche Fluggastdatengesetz konsequent im Sinne der Entscheidung der Richter zu ändern.

Auch die Art. 29-Gruppe wandte sich in einem Schreiben vom 11.4.2018 an die EU-Kommission: Die Fluggastdaten-Richtlinie stehe unzweifelhaft nicht im Einklang mit den EU-Grundrechten und sei umgehend zu ändern.

## Fluggastdatengesetz weiter in Kraft

Trotz der eindringlichen Appelle der Datenschutzbehörden hatte das wegweisende EuGH-Gutachten bisher lediglich zur Folge, dass ein neues Abkommen mit Kanada ausgehandelt wurde. Die umstrittene Fluggastdaten-Richtlinie und auch das darauf beruhende fragwürdige deutsche Fluggastdatengesetz sind nach wie vor in Kraft und in Gebrauch. Die Anwender begrenzen die Auswirkungen des Gutachtens ausschließlich auf das Abkommen mit Kanada. Angesichts der allgemeingültigen Aussagen des EuGH ist dies zu kurzsichtig.

Auseinandersetzung geht weiter

Für die reisenden Personen bedeutet dies zahlreiche Eingriffe in ihr Recht auf Privatsphäre und das Recht auf Schutz ihrer personenbezogenen Daten, welche nicht ausreichend gerechtfertigt sind. Die Auseinandersetzung im Zusammenhang mit der Nutzung von Fluggastdaten geht weiter.

# 1.3 BGH-Urteil: Über den Tod hinaus online?

Stirbt eine Person, die Benutzerkonten auf Online-Plattformen hat, so können die Erben vom jeweiligen Plattformbetreiber verlangen, dass sie Zugang zu dem Profil des Verstorbenen erhalten. Das ergibt sich aus dem Urteil des Bundesgerichtshofs (BGH) vom 12. Juli 2018.

Accounts im Gedenkzustand

Plattformbetreiber verfahren mitunter so, dass sie die Accounts verstorbener Nutzer in einen sogenannten Gedenkzustand versetzen. So können die über die Online-Plattform verbundenen Nutzer je nach Einstellungen des Verstorbenen noch Nachrichten und Kommentare auf dessen Profil hinterlassen. Die Nachrichten und Kommentare, die vor dem Tod des Nutzers auf seinem Profil abrufbar waren, bleiben es weiterhin, allerdings mit einem zusätzlichen Hinweis auf dessen Tod.

## Nutzungsvertrag geht auf Erben über

Der Plattformbetreiber hatte in dem Fall, der dem BGH zur Entscheidung vorlag, den Zugriff für die Erben auf das Benutzerkonto des Verstorbenen gesperrt, obwohl ihnen die Zugangsdaten bekannt waren. Der BGH entschied, dass der Nutzungsvertrag des Nutzers mit seinem Tod auf dessen Erben übergehe und dem Zugang zum Profil weder das postmortale Persönlichkeitsrecht des Verstorbenen noch das Fernmeldegeheimnis noch der Datenschutz entgegenstünden.

## Vereinbarkeit mit fortwirkendem Persönlichkeitsrecht

Der Zugang kann von den Erben nur geltend gemacht werden, wenn der Zugangsanspruch des verstorbenen Nutzers auf die Erben übergeht, also vererbbar ist.

Der BGH führt aus, dass das Persönlichkeitsrecht des Nutzers, das nach seinem Tod im sogenannten postmortalen Persönlichkeitsrecht fortwirkt, keinen Vorrang gegenüber dem Erbrecht habe. Damit stehe es der Vererbung eines Zugangsanspruchs gegenüber dem Plattformbetreiber nicht entgegen.

## Vereinbarkeit mit dem Fernmeldegeheimnis

Der Mitteilung von Zugangsdaten an die Erben durch den Plattformbetreiber stünden auch nicht die Vorschriften zum Schutz des Fernmeldegeheimnisses nach dem Telekommunikationsgesetz entgegen, so der BGH.

Nach § 88 Abs. 3 Telekommunikationsgesetz (TKG) ist es den Anbietern von Telekommunikationsdiensten grundsätzlich verboten, sich oder anderen als den Telekommunikationsteilnehmern Nachrichteninhalte und die näheren Umstände der Telekommunikation mitzuteilen. Ausnahmen hiervon greifen nur, soweit dies nötig

ist, um die Telekommunikation technisch zu ermöglichen oder die technischen Systeme zu schützen. Auch wenn es der Rechtsverfolgung oder Rechtsverteidigung dient, ist damit die Mitteilung von Kommunikationsinhalten zu diesem Zweck an „andere“ grundsätzlich verboten.

Erben sind nicht „andere“

Nach Auffassung des BGH verstoße der Plattformbetreiber nicht gegen § 88 Abs. 3 TKG, wenn er die Zugangsdaten des Verstorbenen den Erben zu diesem Zweck mitteilt. Die Erben seien nicht „andere“ im Sinne dieser Vorschrift. Sie würden vielmehr nach dem Tod des Nutzers dessen Rolle als Telekommunikationsteilnehmer einnehmen.

Die Einordnung der Erben als „andere“ führe zu einer grundlosen Ungleichbehandlung abhängig von Ort und Art der Speicherung der Kommunikationsinhalte. Das Mitteilungsverbot greift nämlich nicht, wenn der Nutzer vor seinem Tod einen Ausdruck der Kommunikation angefertigt oder die Kommunikation bei sich lokal gespeichert hat. In beiden Fällen seien jedoch die Vertraulichkeitsinteressen der Telekommunikationsteilnehmer gleichermaßen schutzwürdig.

Erbrecht hat Vorrang

Gegen die Einordnung der Erben als „andere“ sprächen auch die Vorschriften des Bürgerlichen Gesetzbuchs (BGB), in denen der Übergang von höchstpersönlichen Rechtspositionen, wie persönlichen Schriftstücken, Familienpapieren und Tagebüchern des Verstorbenen, angeordnet werden. Darin komme die gesetzlich gewollte Unterordnung der Vertraulichkeitsinteressen des Verstorbenen und dessen Kommunikationspartnern gegenüber dem Erbrecht zum Ausdruck.

## Vereinbarkeit mit der DS-GVO

Nach Ansicht des BGH sei die Mitteilung der Zugangsdaten an die Erben auch aus Sicht des Datenschutzes nicht zu beanstanden. Datenverarbeitungen, die notwendig sind, um einen Vertrag zu erfüllen oder ein überwiegendes berechtigtes Interesse zu wahren, sind datenschutzrechtlich zulässig.

Das Konto ist maßgebend

- Die Übermittlung und das Bereithalten von Nachrichten zum Abruf und die damit einhergehenden Datenverarbeitungen seien eine wesentliche Vertragspflicht des Plattformbetreibers. Hieran ändere der Tod des ursprünglichen Kontoinhabers nichts, da die Vertragspflicht des Plattformbetreibers an das Konto einer Person und nicht an die Person selbst anknüpfe.
- Die Erforderlichkeit zur Wahrung eines berechtigten Interesses ergebe sich daraus, Ansprüche verfolgen und abwehren zu können, die sich aus dem Erbe ergeben. Ferner sei auch das ideelle Interesse der Erben als berechtigtes Interesse anzuerkennen, mit dem Zugang zu dem Benutzerkonto des Verstorbenen Aufschluss darüber zu erhalten, ob dieser zuvor Suizidabsichten gehabt hat.
- Diesen berechtigten Interessen der Erben stünden Belange der Kommunikationspartner, auch wenn diese minderjährig sind, nicht entgegen. Die Minderjährigkeit als solche führe nicht per se zu einem Überwiegen der Interessen der Kommunikationspartner gegenüber den berechtigten Interessen der Erben.
- Da die Nutzer der Plattform ihre personenbezogenen Daten freiwillig und bewusst an den Plattformbetreiber übermittelten, um sie für ein bestimmtes Benutzerkonto bereit zu stellen, überwiege ihr Interesse an der Vertraulichkeit nicht gegenüber den berechtigten Interessen der Erben.

Kontrollverlust bei Versand der Nachricht

- Dem Absender einer elektronischen Nachricht sei zudem wie einem Absender eines Briefs bewusst, dass er nach dem Versand der Nachricht nicht mehr kontrollieren könne, welche Person letztlich von deren Inhalt Kenntnis nimmt.
- Ferner sei es für die Kommunikationspartner absehbar, dass nach dem Tod eines Kontoinhabers dessen Erben Kenntnis von den Daten erhalten können.

## Rechte des Nutzers und Rechte des Betroffenen

Gegenstand der Entscheidung des BGH war allein die Frage der Vererbbarkeit der Rechte des Nutzers aus dem Nutzungsvertrag mit dem Plattformbetreiber und die Durchsetzbarkeit dieser vertraglichen Rechte der Erben. Damit blieb die nach wie vor strittige Frage unbeantwortet, ob die gesetzlichen Rechte des Betroffenen nach der DS-GVO vererbbar sind.

Nicht nur das Persönlichkeitsrecht im Allgemeinen, sondern auch das Recht auf informationelle Selbstbestimmung im Speziellen, das den wesentlichen Teil der verfassungsmäßigen Grundlage für das Datenschutzrecht bildet, sind über den Tod hinaus schutzwürdig.
Die Zukunft wird zeigen, inwieweit diese Schutzwürdigkeit im Ergebnis dazu führt, dass die Erben die Rechte, die der Nutzer vor seinem Tod als Betroffener nach der DS-GVO geltend machen konnte, in zumindest entsprechender Weise geltend machen können. Eines steht jedenfalls schon jetzt fest: Die DS-GVO selbst enthält keine Regelung, nach der die Rechte des Betroffenen mit dessen Tod auf seine Erben übergehen.

# F.2. Beteiligung an Gesetzgebungsverfahren

## 2.1 Hitzige Diskussionen um das neue Polizeigesetz

Im Mai 2018 haben die niedersächsischen Regierungsfraktionen ein Reformgesetz zum Gefahrenabwehrrecht in den Landtag eingebracht. Dieses sah zahlreiche neue Befugnisse zur Datenerhebung für die Polizei vor, von denen einige tief in die Privatsphäre der Bürgerinnen und Bürger eingreifen. Ich habe deshalb scharfe Kritik an Teilen des Gesetzesentwurfs geäußert.

Eine der neuen Befugnisse zur Verhütung von Straftaten ist das Instrument der sog. Quellen-Telekommunikationsüberwachung. Damit wird zukünftig auch das Abhören verschlüsselt stattfindender Telekommunikation möglich. Außerdem soll die Polizei zur Verhütung terroristischer Straftaten mit Hilfe der Online-Durchsuchung Daten von Privatrechnern ohne Wissen des Betroffenen auslesen können.

Ausdehnung der Videoüberwachung

Weiterhin sieht der Gesetzentwurf vor, die Videoüberwachung im öffentlichen Raum umfassend neu zu regeln und auszuweiten. Bisher sind Bildaufzeichnungen nur zulässig, wenn an dem videoüberwachten Ort schwere Straftaten begangen wurden. Zukünftig sollen schon geringfügige Straftaten ausreichen. Zudem können Polizeibeamte zukünftig Körperkameras (Bodycams) tragen und in Konfliktsituationen einschalten.

Der Landtag hat im Rahmen einer öffentlichen Anhörung am 9. August 2018 zahlreichen Verbänden Gelegenheit gegeben, zum Gesetzentwurf Stellung zu nehmen. Hiervon habe ich Gebrauch gemacht und sowohl schriftlich als auch mündlich zahlreiche datenschutzrechtliche Bedenken vorgetragen. Die wesentlichen Kritikpunkte waren:

### Begründung zu pauschal

Die Begründung für die vorgeschlagenen Gesetzesänderungen, die teilweise tief in die Privatsphäre der Bürgerinnen und Bürger eingreifen, ist durchgängig oberflächlich und beschränkt sich pauschal auf das übergeordnete Ziel der

Keine nachvollziehbare Diskussion

Bekämpfung des Terrorismus. Somit kann keine für die Öffentlichkeit und den Gesetzgeber nachvollziehbare Diskussion in Gang gesetzt werden. Diese ist aber erforderlich, um eine angemessene Abwägung zwischen den Sicherheitsinteressen des Staates einerseits und den Freiheitsrechten der Bürgerinnen und Bürgerinnen andererseits vornehmen zu können.

GBD bestätigt Kritik

Diese grundlegende Kritik am Gesetzentwurf stieß zunächst auf wenig Verständnis. Die weiteren Ausschussberatungen und vor allem die schriftlichen Ausführungen des Gesetzgebungs- und Beratungsdienstes haben hingegen deutlich belegt, dass ich den Begründungsmangel zu Recht gerügt habe. Die Notwendigkeit vieler Änderungen konnte das zuständige Innenministerium häufig nur auf Nachfrage der Abgeordneten im Nachhinein und an vielen Stellen gar nicht mit Fällen aus der Praxis belegen. In der Folge wurde beispielsweise der Katalog zur Definition der „terroristischen Straftaten“ und damit die Eingriffsmöglichkeiten für die entsprechenden Befugnisse erheblich eingeschränkt.

## Fehlender Richtervorbehalt

An vielen Stellen nachgebessert

Für zahlreiche neue Befugnisse, etwa für die elektronische Fußfessel, enthält der Gesetzentwurf nur ungenügende Regelungen, wie das jeweilige Verfahren ordnungsgemäß ablaufen muss. An vielen Stellen des Gesetzes wurde inzwischen entsprechend meinen Forderungen nachgebessert, sodass nur ein Richter Maßnahmen wie die elektronische Fußfessel, längerfristige Meldeauflagen oder Kontakt- und Aufenthaltsvorgaben anordnen kann.

## Videoüberwachung zu stark ausgeweitet

Bei der Videoüberwachung formuliert der Gesetzentwurf die Voraussetzung für den Einsatz zur Gefahrenabwehr und Verhütung von Straftaten auf öffentlichen Straßen und Plätzen zwar bestimmter als bisher. Jedoch weitet er die Videoüberwachung in bedenklicher Weise aus, indem zukünftig in jedem Fall der Beobachtung durch eine Kamera auch aufgezeichnet werden kann.

Nur Live-Bilder verhindern Straftaten

Ich halte an meiner Aussage fest, dass eine Videobeobachtung im öffentlichen Raum nur dann sinnvoll ist, wenn jemand das Geschehen live mitverfolgt und bei Gefahr sofort Hilfe organisieren kann. Bildaufzeichnungen sind dafür nicht geeignet. Sie dienen in erster Linie der Strafverfolgung und haben damit im Gefahrenabwehrrecht nur nachrangig Platz. Die Erweiterung der Bildaufzeichnungsmöglichkeiten geht damit in die falsche Richtung.

## Verdeckte Videoüberwachung

Keine abschreckende Wirkung durch versteckte Kameras

Ebenfalls kritikwürdig ist es, dass der Gesetzentwurf an der verdeckten Maßnahme der Bildaufzeichnung trotz verfassungsrechtlicher Bedenken festhält. Eine derartige Regelung findet sich nur noch in Rheinland-Pfalz. Wie eine Kamera, die für die betroffenen Personen nicht erkennbar ist, abschreckende Wirkung entfalten und von Straftaten abhalten soll, bleibt weiterhin ungeklärt. Die verdeckte Anfertigung von Bildaufzeichnungen ist eindeutig dem Bereich der Strafverfolgung zuzuordnen, weshalb dem Landesgesetzgeber die Gesetzgebungsbefugnis fehlt.

## Staatstrojaner nutzen Sicherheitslücken

Die besonders eingriffsintensiven neuen Maßnahmen der Quellen-Telekommunikationsüberwachung und Online-Durchsuchung werfen viele tatsächliche und verfassungsrechtliche Fragen auf, die der Gesetzentwurf nicht ausreichend beantwortet. Für beide Formen der Datenerhebung ist es nötig, dass staatliche Behörden eine Software (Staatstrojaner) ohne Kenntnis der Betroffenen auf Smartphone oder Computer installieren. Hierfür muss die Polizei auf bekannte Sicherheitslücken in den Betriebssystemen zurückgreifen, die auch von Kriminellen genutzt werden können. Dieses Verhalten steht im Widerspruch zur staatlichen Pflicht, die Bürgerinnen und Bürger wirksam vor Cyberangriffen zu schützen.

Auch ist es problematisch, dass der Staatstrojaner grundsätzlich sämtliche Daten der betroffenen Person auslesen kann. Dies wäre in jedem Fall unverhältnismäßig und damit verfassungswidrig. Technisch muss daher sichergestellt sein, dass der Staatstrojaner nur in einem begrenzten Umfang auf bestimmte Daten zugreifen kann. Ob der Gesetzgeber diese Vorgabe überhaupt wirksam formulieren kann, um einen missbräuchlichen Einsatz durch die Polizei zu verhindern, bleibt eine offene verfassungsrechtlich bedeutsame Frage, auf die der Gesetzentwurf keine Antwort gibt.

Missbrauch von Trojanern verhindern

## Andere Bundesländer machen es besser

Schließlich muss der Gesetzentwurf an zahlreichen Stellen ergänzt werden, um das Datenschutzniveau anderer Ländergesetze zum Polizeirecht zu erreichen. Bereichsspezifische Regelungen zur Zweckänderung und Löschung von Daten fehlen fast durchgängig, so beispielsweise bei der Videoüberwachung und Rasterfahndung. Unterschiedlichen Höchstspeicherfristen für bestimmte Personengruppen wie Kontakt- und Begleitpersonen, Zeugen oder Opfer wären wünschenswert. In anderen Ländern wie Bayern, Baden-Württemberg, Berlin, Brandenburg, Hessen oder Nordrhein-Westfalen ist dies bereits Standard.

## Positive Aspekte des Gesetzentwurfs

Der Gesetzentwurf setzt jedoch an einigen Stellen auch Forderungen um, die ich erhoben habe. So wird z. B. eine ausdrückliche Rechtsgrundlage für die Abschnittskontrolle zur Geschwindigkeitsüberwachung (Section Control) geschaffen. Ferner wird es gesetzliche Regelungen zur Videoüberwachung zum Zweck der Verkehrslenkung geben und zur Überwachung von Personen, die sich im Polizeigewahrsam befinden. Auch werden die sog. Bodycams der Polizei erstmals in Niedersachsen auf eine ausreichende gesetzliche Grundlage gestellt.

Rechtsgrundlagen für Section Control und Bodycams

Zum Redaktionsschluss dieses Berichts war das parlamentarische Verfahren noch nicht beendet. Ich werde dieses Thema daher in meinem nächsten Tätigkeitsbericht wieder aufgreifen.

# 2.2 Gesetzentwurf zu digitaler Verwaltung und Informationssicherheit mit Schwächen

Mit dem „Gesetz zur Förderung und zum Schutz der digitalen Verwaltung in Niedersachsen und zur Änderung des Niedersächsischen Beamtengesetzes[1]“ sollen Verwaltungsmodernisierung und Bürokratieabbau gefördert und die Grundlage für eine moderne IT-Sicherheitsarchitektur in der niedersächsischen Verwaltung geschaffen werden. Allerdings sieht der Gesetzentwurf der Landesregierung zur Wahrung der Informationssicherheit weitreichende Eingriffsbefugnisse vor. Ich habe deshalb an verschiedenen Stellen deutliche Nachbesserungen zum Schutz der Betroffenen gefordert.

Für mich war insbesondere das in dem Entwurf enthaltene Niedersächsische Gesetz über digitale Verwaltung und Informationssicherheit (NDIG) von großer Relevanz. Es enthält Normen zur digitalen Verwaltung und zur Gewährleistung der Informationssicherheit.

Neuwahl stoppt vorheriges Verfahren

Schon vor dem Entwurf des NDIG gab es Ansätze, die Informationssicherheit in der Landesverwaltung gesetzlich zu regeln. Ein entsprechender Gesetzentwurf wurde von mir mit einer Stellungnahme begleitet. Aufgrund der vorzeitigen Neuwahlen des Niedersächsischen Landtags wurde dieses Gesetzgebungsverfahren jedoch nicht mehr beendet.

## IT-Sicherheit und Datenschutz miteinander vereinbaren

Reaktion auf ständig neue Bedrohungslagen

Dass die beiden Bereiche Informationssicherheit und digitale Verwaltung im Entwurf des NDIG gemeinsam geregelt werden, überrascht nicht. Die Gewährleistung der Informationssicherheit bei den niedersächsischen Behörden ist eine datenschutzrechtliche Notwendigkeit. Es handelt sich um eine anspruchsvolle Aufgabe, weil die Analyse von und Reaktion auf ständig neue Bedrohungslagen erforderlich ist. Der Entwurf des Gesetzes zeigt aber auch, dass Anforderungen der Informationssicherheit und des Datenschutzes nicht immer einfach miteinander zu vereinbaren sind.

Der Entwurf des NDIG erlaubt es Behörden, die mit dem Landesdatennetz verbunden sind, zur Abwehr von Gefahren für die IT-Sicherheit umfangreiche automatisierte und nichtautomatisierte Datenauswertungen vorzunehmen. Es kann zu Auswertungen von Daten kommen, die auf mit dem Landesdatennetz verbundenen IT-Systemen gespeichert werden. Ebenso kann an Übergabe- und Knotenpunkten des Landesdatennetzes nach auffälligem Datenverkehr gesucht werden.

---

[1] Der Entwurf kann unter https://www.niedersachsen.de/download/135936/Entwurf_Gesetz_zur_Foerderung_und_zum_Schutz_der_digitalen_Verwaltung_in_Niedersachsen_und_zur_Aenderung_des_Niedersaechsischen_Beamtengesetzes.pdf abgerufen werden.

## Auswertung der Inhaltsdaten möglich

Aus Sicht des Datenschutzes ist besonders bedenklich, dass der Datenverkehr auch entschlüsselt werden kann und eine Auswertung der Inhaltsdaten möglich ist. Von dieser können sowohl Bürger, die mit Behörden kommunizieren, als auch die Mitarbeiterinnen und Mitarbeiter in den Behörden betroffen sein. Die vorgesehenen Maßnahmen besitzen also eine erhebliche Eingriffstiefe. Hierfür sollen Systeme zur automatisierten Erkennung von Angriffen und zur Analyse der Sicherheitslage, sogenannte Intrusion Detection Systems (IDS) und Security Incident and Event Management Systems (SIEM), eingesetzt werden.

Sowohl Bürger als auch Beschäftigte betroffen

## Gesetzentwurf muss nachgebessert werden

Gegenüber der Landesregierung habe ich deutlich gemacht, dass ich die Gewährleistung der Informationssicherheit als unverzichtbares Ziel sehe und anerkannt, dass der Einsatz von modernen Systemen hierfür erforderlich ist. Bei den geplanten, tiefgreifenden Eingriffen ist es aber besonders wichtig, dass ein möglicher Miss- oder Fehlgebrauch verhindert wird. Um die Verhältnismäßigkeit zu wahren, ist es daher insbesondere erforderlich, den Gesetzesentwurf mindestens in folgenden Punkten nachzubessern:

- Die Befugnisnorm muss im Hinblick auf das geplante Einsatzszenario so spezifisch sein, dass durch technologische Entwicklungen bei IDS und SIEM keine schwerwiegenden Grundrechtseingriffe zu befürchten sind.

- Die Norm hat sicherzustellen, dass durch fachkundiges Personal beurteilt wird, wann Gefahren für die IT-Sicherheit vorliegen, die entsprechende Eingriffe rechtfertigen. Nach dem Entwurf kann jede Behörde, die mit dem Landesdatennetz verbunden ist, von den Auswertungsbefugnissen Gebrauch machen.

- Die Erstellung von personenbezogenen Profilen zur Vorhersage des Nutzungsverhaltens natürlicher Personen ist explizit zu untersagen. Es gibt IDS-Funktionen, die Auffälligkeiten erkennen, indem sie analysieren, ob das aktuelle Nutzerverhalten vom bislang gezeigten abweicht. Solche Anomalien sollen dann ein Hinweis auf eine Gefahr für die IT-Sicherheit sein.

  Keine Erstellung von personenbezogenen Profilen

- Es ist festzulegen, dass eine manuelle Auswertung von Kommunikationsinhalten dem Richtervorbehalt unterliegt. Bei einem so schwerwiegenden Grundrechtseingriff ist ein effektiver Schutz der Rechte der betroffenen Personen nur dann möglich, wenn dies durch eine unabhängige und neutrale Instanz geschieht. Die bislang vorgesehene Anordnung durch die Behördenleitung und einen Beschäftigten mit der Befähigung zum Richteramt erfüllt diese Voraussetzung nicht.

Das Gesetzgebungsverfahren wurde im Berichtszeitraum nicht abgeschlossen. Ich werde, wenn nötig, meine Bedenken gegenüber dem Gesetzgeber erneut anbringen.

# 2.3 Informationsfreiheitsgesetz für Niedersachsen scheitert auf der Zielgeraden

Langwierig aber letztlich ergebnislos wurde in den vergangenen Jahren in Niedersachsen um ein Informationsfreiheitsgesetz (IFG) gerungen. Seit den ersten Entwürfen im Jahr 2001 gab es in jeder Legislaturperiode erneute Anläufe, um ein IFG auf den Weg zu bringen. Doch entweder wurden die Pläne nicht weiter verfolgt oder das jeweilige Projekt scheiterte im Gesetzgebungsverfahren.

Fast alle Bundesländer haben ein IFG

Während der niedersächsische Gesetzgeber in 18 Jahren ein ums andere Mal scheiterte, haben (bis auf Bayern und Sachsen) alle anderen Bundesländer sowie der Bund eigene Gesetze zur Informationsfreiheit verabschiedet. Einige Länder, so etwa Hamburg, Rheinland-Pfalz oder Bremen haben inzwischen bereits weiterentwickelte Gesetze, die neben dem antragsgebundenen Informationszugang auch die Informationsbeschaffung über ein Online-Transparenzportal ermöglichen.

Die neuen Transparenzgesetze schreiben dabei vor, welche Informationen proaktiv von den öffentlichen Stellen in das Portal einzustellen sind. Bürger können so einfach online auf die gewünschten Informationen zugreifen. So werden nicht nur Zeit und Verwaltungsaufwand, sondern auch Gebühren der Bürger gespart.

## Open Data Kampagne in Niedersachsen

Statt ein erneutes Gesetzgebungsverfahren für ein IFG anzustoßen, versucht sich Niedersachsen derzeit an einem anderen Ansatz. Mit einer „Open Data Kampagne“ sollen der Öffentlichkeit landeseigene Daten digital bereitgestellt werden. Welche Art von Daten im Detail dabei eigesehen werden können, soll von einer Task Force definiert werden.

Open Data Strategie kann IFG nicht ersetzen

Genau hier liegt der entscheidende Unterschied zur Rechtslage unter einem IFG. Auf einer solchen Gesetzesgrundlage würde nicht mehr die Verwaltung den potenziellen Mehrwert einer Information für Bürger und Unternehmen prognostizieren, sondern das Recht auf Zugang zu Informationen würde anlasslos allen Informationssuchenden offenstehen. Im Sinne einer Beweislastumkehr könnte die Verwaltung ihrerseits ein Informationsgesuch nur ablehnen, wenn im IFG normierte Ausnahmetatbestände entgegenstehen. Eine umfassenden Open Data Strategie benötigt also ein IFG als Grundlage und kann nicht losgelöst in einer landespolitischen Kampagne betrieben werden.

## Neuwahlen stoppen guten Gesetzentwurf

Die aktuelle Strategie der Landesregierung ist auch deshalb bedauerlich, weil insbesondere der Entwurf eines niedersächsischen Informationszugangsgesetzes aus dem Jahr 2017 (Drucksache 17/8004) aus Sicht des Datenschutzes durchaus zufriedenstellend war. In der Summe konnte ich im Rahmen der Verbandsanhörung feststellen, dass der damalige Entwurf den Schutz personenbezogener Daten und damit die Persönlichkeitsrechte Betroffener in ausreichendem Maße berücksichtigt und schützt. Meine weiterführenden Vorschläge, insbesondere zur Gewährleistung von Normenklarheit und Praxistauglichkeit bei der damals vorgesehenen Einrichtung einer / eines Beauftragten für die Informationsfreiheit, dessen Aufgaben durch mein Haus hätten wahrgenommen werden sollen, wären sicher im weiteren Verlauf diskutiert worden. Doch das vorzeitige Ende der Legislaturperiode stoppte das Gesetzgebungsverfahren wie auch 60 weitere Entwürfe abrupt.

## Verhaltene Formulierung im Koalitionsvertrag

Die neue Regierung hat in Ihrem Koalitionsvertrag 2017 – 2022 leider eine äußerst verhaltene Formulierung für ihren weiteren Umgang mit dem Thema Informationsfreiheitsgesetz gewählt. Dort heißt es lediglich: „Wir wollen die Erfahrungen anderer Bundesländer mit einem Informationsfreiheits-und Transparenzgesetz evaluieren und auf der Grundlage dieser Ergebnisse über die Einführung eines Informationsfreiheits- und Transparenzgesetzes in Niedersachsen entscheiden."

Zunächst Erfahrungen anderer Länder evaluieren

## 2.4 Novellierung des Niedersächsischen Justizvollzugsgesetzes

Die Landesregierung hat einen Gesetzentwurf zur Novellierung des Niedersächsischen Justizvollzugsgesetzes (NJVollzG) erarbeitet und im Dezember 2018 ins Kabinett eingebracht. Meine Behörde wurde bereits frühzeitig im Rahmen der Ressortabstimmung beteiligt. Ausgangspunkt der Gesetzesänderung ist vor allem der Anpassungsbedarf, der durch die europäische Datenschutzreform entstanden ist.

Ziel des Gesetzes ist es, u. a. die Richtlinie (EU) 2016/680 (genannt JI-Richtlinie) in den datenschutzrechtlichen Bestimmungen des NJVollzG umzusetzen. Zudem sollen die Forderungen aus dem aktuellen Koalitionsvertrag erfüllt werden. So wird die elektronische Aufenthaltsüberwachung für Gefangene (elektronische Fußfessel) eingeführt. Ferner schafft der Gesetzentwurf eine Ermächtigungsgrundlage für die Anordnung einer Fixierung von Inhaftierten und setzt damit die jüngste Rechtsprechung des Bundesverfassungsgerichts um (Urteil vom 24. Juli 2018; 2 BvR 309/15, 2 BvR 502/16).

Nähere Informationen zur JI-Richtlinie finden Sie auch auf Seite 37

## Neuerungen für Haftanstalten

Eine datenschutzrechtlich relevante Neuerung stellt zunächst die elektronische Fußfessel für Gefangene dar. Diese können die Vollzugsanstalten nun im Rahmen von Lockerungen des Vollzuges nutzen. Ihre Einführung ist Bestandteil des aktuellen Koalitionsvertrags zwischen SPD und CDU. Mit der elektronischen Fußfessel soll der Opferschutz verbessert werden. Die Wohnungen der betroffenen Gefangenen bleiben aber als Kernbereich der privaten Lebensgestaltung von der Datenerhebung ausgenommen. Das heißt, die Fußfessel überträgt von dort keine Daten.

Einführung der elektronischen Fußfessel

Der Gesetzentwurf enthält darüber hinaus eine Ermächtigungsgrundlage für die Datenerhebung bei Dritten (z. B. über Besucher des Gefangenen). Eine solche ist im Zweiten Teil des Niedersächsischen Datenschutzgesetzes nicht enthalten, so dass es hier einer bereichsspezifischen Regelung bedarf.

Ebenfalls wurde im Gesetz eine Ermächtigungsgrundlage für das Auslesen von elektronischen Datenspeichern geschaffen. Dabei geht es um Speichergeräte, die sich entweder ohne Erlaubnis in der Haftanstalt bei einer inhaftierten Person befinden oder solche, die in den allgemein zugänglichen Räumen oder auf dem Gelände der Vollzugsanstalt aufgefunden werden, ohne einer Person zugeordnet werden zu können. Um sie auslesen zu dürfen, bedarf es jeweils einer einzelfallbezogenen Güterabwägung (zwischen den Sicherheitsinteressen der Anstalt und dem Recht auf informationelle Selbstbestimmung) sowie der schriftlichen Anordnung der Anstaltsleitung. Ich begrüße diese Regelung sehr, weil die Haftanstalt dadurch nicht pauschal auf alle Speichermedien zugreifen kann, sondern den jeweiligen Einzelfall betrachten muss.

## Frühzeitige Einbindung des Datenschutzes

Erfreulicherweise wurden bereits im Rahmen der Ressortabstimmung Vorschläge meines Hauses in den Gesetzentwurf aufgenommen. Dazu zählt etwa eine Regelung zum Kernbereichsschutz im Zusammenhang mit dem Auslesen von Datenspeichern sowie nach unterschiedlichen Personengruppen differenzierende Kontrollfristen für die Erforderlichkeit der Speicherung personenbezogener Daten. So sind die Speicherfristen für Besucher etwa kürzer als für Gefangene. Auch die Gesetzesbegründung wurde an verschiedenen Stellen auf mein Anraten hin konkretisiert und ergänzt.

Auslesen von Speichermedien nur mit schriftlicher Anordnung

Das bevorstehende parlamentarische Verfahren wird von meinem Haus aufmerksam verfolgt werden, um auf eine weiterhin konsequente Berücksichtigung der datenschutzrechtlichen Grundsätze hinzuwirken. Insgesamt ist das bisherige Verfahren ein positives Beispiel für die gelungene Zusammenarbeit zwischen Landesregierung und Aufsichtsbehörde.

Unterschiedliche Fristen für Besucher und Gefangene

# 2.5 Rundfunk und die DS-GVO – der NDR-Datenschutz-Staatsvertrag

Wie in vielen anderen Rechtsgebieten mussten auch die Datenschutzvorschriften für den öffentlich-rechtlichen Rundfunk an die Datenschutz-Grundverordnung angepasst werden. Die Länder Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein trafen die erforderlichen Regelungen im „Staatsvertrag über den Datenschutz beim Norddeutschen Rundfunk" (NDR-Datenschutz-Staatsvertrag), der nun den Rundfunk-Staatsvertrag ergänzt.

Stellungnahme der betroffenen Bundesländer

Im Rahmen der Verbandsbeteiligung gab ich im Namen der Landesdatenschutzbeauftragten der betroffenen Bundesländer eine gemeinsame Stellungnahme ab. Von grundsätzlicher Bedeutung war in diesem Zusammenhang die Neuregelung des sogenannten Medienprivilegs – eine weitgehende Entbindung des Rundfunks von den Datenschutzvorschriften der Datenschutz-Grundverordnung (DS-GVO) bei der Verarbeitung von personenbezogenen Daten zu journalistischen Zwecken. Diese Ausnahme vom Datenschutzrecht muss den Vorgaben von Art. 85 DS-GVO genügen (siehe dazu auch Seite 33).

In der Stellungnahme zum NDR-Datenschutz-Staatsvertrag wies ich nachdrücklich darauf hin, dass die europäischen Vorgaben zwingend zu berücksichtigen sind. Dies schließt es aus, das zuvor im Rundfunk-Staatsvertrag geregelte Medienprivileg in der damaligen Form beizubehalten. Der NDR-Datenschutz-Staatsvertrag lässt aber deutlich erkennen, dass genau diese Intention verfolgt wurde.

## Vertrag geht weit über Erforderlichkeit hinaus

Durch den NDR-Datenschutz-Staatsvertrag werden zahlreiche Vorschriften der DS-GVO ohne Begründung und weit über die Erforderlichkeit zur Gewährleistung der freien journalistischen Tätigkeit hinaus für nicht anwendbar erklärt. Die darin enthaltenen Ausführungen lassen es insbesondere vermissen, dass eine Interessenabwägung zwischen dem Datenschutz und der Meinungs- und Informationsfreiheit überhaupt stattgefunden hat.

Ausnahmen für Pressefreiheit unbedingt erforderlich

Ich möchte hier nicht missverstanden werden: Ich halte es zur Gewährleistung der verfassungsrechtlich garantierten Presse- und Rundfreiheit für unbedingt erforderlich, dass es Ausnahmevorschriften von der DS-GVO für journalistische Zwecke gibt. Allerdings nur insoweit sie für die journalistische Tätigkeit auch zwingend erforderlich sind.

## Datenschutz teilweise verschlechtert

Neben dieser grundsätzlichen Kritik, habe ich im Detail zu den einzelnen Vorschriften des Entwurfs Stellung genommen. Bedauerlich war aus meiner Sicht vor allem, dass einzelne Regelungen des Entwurfs gegenüber den bisherigen Datenschutzvorschriften eine Verschlechterung darstellten. Im Ergebnis muss ich leider feststellen, dass meine wesentlichen Bedenken nicht berücksichtigt wurden.

## 2.6 Anpassungen an Presse- und Mediengesetz

Neben den Datenschutzvorschriften für den Rundfunk mussten auch die landesrechtlichen Vorschriften für die weiteren Medien an die Datenschutz-Grundverordnung angepasst werden. Das Niedersächsische Presse und das Niedersächsische Mediengesetz wurden – zusammen mit zahlreichen anderen Landesgesetzes – durch das Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts neu geregelt. Ich habe die Verbandsbeteiligung genutzt, um ausführlich Stellung zu nehmen und Verbesserungsvorschläge einzubringen.

Die Datenschutzvorschriften des Niedersächsischen Pressegesetzes gelten grundsätzlich für Personen, die für Unternehmen der Presse oder deren Hilfsunternehmen tätig sind. Die Regelungen des Mediengesetzes adressieren die privaten Rundfunkanstalten und Datenverarbeitungen durch vergleichbare Anbieter von Telemedien – also vor allem von journalistischen Veröffentlichungen im Internet. Sie stehen somit in enger Verbindung mit dem NDR-Datenschutz-Staatsvertrag. Alle Gesetze zusammen regeln den Datenschutz für die Medien.

## Alter Wein in neuen Schläuchen

Die Kritikpunkte an den geplanten Datenschutzvorschriften im Presse- und Mediengesetz entsprachen weitgehend denjenigen, die ich auch gegenüber dem NDR-Datenschutz-Staatsvertrag vorgetragen hatte (siehe Seite 66). Der Landesgesetzgeber hatte den Vorgaben von Art. 85 DS-GVO (Siehe Seite 33) keine Rechnung getragen und versucht, alten Wein in neuen Schläuchen zu verkaufen. Darüber hinaus gab es auch bei diesen beiden Gesetzentwürfen aus der Perspektive des Datenschutzes zahlreiche Formulierungen zu bemängeln.

Im Einzelnen machte ich konkrete Verbesserungsvorschläge

Vorschläge zur Verbesserung der Entwürfe

- zu den Vorschriften zum Datengeheimnis,
- zur Reichweite des Medienprivilegs,
- zur Beschränkung der Haftung bei Datenschutzverstößen,
- zur sehr starken Beschränkung der Betroffenenrechte und
- zur Regelung der Datenschutzkontrolle.

## Auch Journalisten müssen Sicherheit gewährleisten

Ziel des Datenschutzes ist es nicht, journalistische Tätigkeiten zu erschweren. Nichtsdestotrotz kann und darf auch in diesem Anwendungsbereich der Schutz der von der Verarbeitung betroffenen Personen nicht unverhältnismäßig gekürzt werden. Es ist z. B. nicht ersichtlich, warum Journalisten nicht dazu verpflichtet sein sollten, den Grundsatz der Richtigkeit der Daten zu beachten sowie die Sicherheit der Verarbeitung durch technische und organisatorische Maßnahmen zu gewährleisten. Ihre journalistische Tätigkeit wird durch diese Anforderungen nicht beeinträchtigt, sondern im Gegenteil eher gefördert.

Einige meiner Änderungsvorschläge haben Eingang in das Niedersächsische Presse- und das Niedersächsische Mediengesetz gefunden. Meine wesentlichen Kritikpunkte blieben aber ungehört.

Wesentliche Kritik bleibt ungehört

# 2.7 Mangelhafter Datenschutz im neuen Schulgesetz

Gleichzeitig zur Neuordnung des Niedersächsischen Datenschutzrechts (siehe Seite 30) wurde auch das Niedersächsische Schulgesetz geändert. Doch statt ausgewogene Regeln zum Umgang mit personenbezogener Daten von Schülerinnen und Schülern zu schaffen, wurden unverhältnismäßige Datenübermittlungen ermöglicht.

Jugendliche beim Wechsel in den Beruf unterstützen

Das Ziel der Novelle des Schulgesetzes ist es, die Zusammenarbeit zwischen den Agenturen für Arbeit, den Trägern der Jugendhilfe und den Trägern der Grundsicherung für Arbeitssuchende sowie den Schulen, Schulbehörden und Schulträgern zu intensivieren. So sollen Jugendliche beim Wechsel in den Beruf unterstützt werden.

## Zu unbestimmt und unverhältnismäßig

Es bleibt unklar, wer Unterstützung benötigt

Ich habe sowohl der Landesregierung als auch dem Landtag mitgeteilt, dass die getroffene Regelung zu unbestimmt und damit unverhältnismäßig ist. Unklar ist vor allem, in welchen Fallkonstellationen überhaupt eine Meldung an welche Institution gehen muss. So wird nicht bestimmt, welche Personen eine Unterstützungsmaßnahme benötigen. Die Regelung birgt damit die Gefahr, dass die Schulen die Eckdaten sämtlicher Schülerinnen und Schüler pauschal an die betreffenden Institutionen melden. In diesem Fall würden erhebliche Datenmengen auch solcher Schülerinnen und Schülern weitergegeben, bei denen keine Zweifel an einem erfolgreichen Schulabschluss und damit keine Gefahr durch Jugendarbeitslosigkeit bestehen.

## Kritik am Gesetz bleibt unbeachtet

Gefahr von Datenfriedhöfen

Durch diese ungefilterte Sammlung nicht benötigter Daten besteht die Gefahr der Produktion von „Datenfriedhöfen“, die letztlich die Arbeit der Behörden eher behindern als sie zu unterstützen. Zudem könnte die automatische Meldung der Daten möglicherweise zu Akzeptanzproblemen bei Schülerinnen und Schülern mit Unterstützungsbedarf führen, wenn ihre Daten ohne Zustimmung beispielsweise an die Agentur für Arbeit übermittelt werden und diese dann unvermittelt Beratungsangebote macht.
Aus diesen Gründen halte ich die Regelung im Schulgesetz für ungeeignet.

Geeignete Alternative bereits vorhanden

Die Regelung ist auch nicht erforderlich, da durch die etablierte Berufsberatung in den Schulen bereits eine geeignete datenschutzfreundliche Alternative vorhanden ist.
Leider wurden meine Bedenken im Gesetzgebungsverfahren allerdings nicht aufgegriffen.

Sensible Gesundheitsdaten

Bei der Auseinandersetzung mit dem Gesetz ist mir darüber hinaus aufgefallen, dass im Schulalltag regelmäßig besonders sensible Gesundheitsdaten verarbeitet werden. Beispielsweise im Rahmen von Schularztuntersuchungen. Ich habe deshalb darauf hingewiesen, dass diese Art der Datenverarbeitung einer konkreten Regelung bedarf, die den Vorgaben der Datenschutz-Grundverordnung gerecht wird. Doch auch in diesem Fall wurde meinen Empfehlungen nicht gefolgt.

# F.3. Polizei und Verfassungsschutz

## 3.1 Dauerthema TKÜ-Anlage – Mängel seit 2012

Seit dem Tätigkeitsbericht für die Jahre 2011 und 2012 berichte ich alle zwei Jahre über erhebliche datenschutzrechtliche Mängel im technisch-organisatorischen Datenschutz bei der polizeilichen Telekommunikationsüberwachung. Diese Mängel sind Ende 2018 bedauerlicherweise immer noch vorhanden.

Nicht nur Zielpersonen betroffen

Die polizeiliche Telekommunikationsüberwachung (TKÜ) zur Strafverfolgung oder Gefahrenabwehr greift besonders tief in die Grundrechte der Betroffenen ein. Erfasst von der Maßnahme sind nicht nur die Zielpersonen (z. B. der Beschuldigte in einem Strafverfahren), sondern auch die übrigen Kommunikationsteilnehmer. Daher ist die Datenverarbeitung im Rahmen einer TKÜ-Maßnahme der höchsten Schutzstufe zuzurechnen, die Anforderungen an den technisch-organisatorischen Datenschutz sind dementsprechend besonders hoch.

Zusammenarbeit mit der LfDI Bremen

Die vom Landeskriminalamt (LKA) Niedersachsen – auch für das Land Bremen – betriebene TKÜ-Anlage weist jedoch nach wie vor erhebliche datenschutzrechtliche Mängel auf. Die seit 2012 ausstehende Beseitigung dieser Mängel habe ich in den vergangenen beiden Jahren erneut eingefordert. Dies geschah zum einen in eigener Landeszuständigkeit, zum anderen in Abstimmung mit der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (LfDI Bremen).

### Die Defizite im Einzelnen

In verschiedenen Analysen, teilweise gemeinsam mit der LfDI Bremen, kritisierte ich die teils erheblichen Defizite bei der Umsetzung der datenschutzrechtlichen Anforderungen. Die zum Teil erst auf Anforderung bei meiner Behörde eingereichten Unterlagen zum Verfahren umfassten 20 Dokumente vor allem zu den für IT-Verfahren üblichen Aspekten:

Dokumente für IT-Verfahren

- Verfahrensbeschreibung,
- Vertragsausgestaltung,
- Betriebskonzept,
- Teilaussagen zum Schutzbedarf und zur Risikobewertung,
- Benutzer- und Rollenkonzept,
- IT-Sicherheitskonzeption,
- Wartung und IT-Infrastruktur.

Zusätzlich gab es spezifische Dokumente zur Regelung der Datenlöschung im Kernbereich privater Lebensgestaltung sowie zur Mandantentrennung für verschiedene Polizeibehörden und -dienststellen.

## Umfassender Mängelkatalog

Austausch mit dem Innenministerium ohne Ergebnisse

Nach intensiver Prüfung der vorliegenden Unterlagen stellte ich eine Reihe von Datenschutzmängeln fest. Zum Zeitpunkt der mit der LfDI Bremen gemeinsamen durchgeführten Prüfung befand sich die TKÜ-Anlage bereits im Wirkbetrieb. Das Ministerium für Inneres und Sport wurde erstmals im August 2013 über die bestehenden Mängel informiert. In der Folgezeit fanden mehrere Gespräche mit dem Innenministerium statt, allerdings ohne greifbare Ergebnisse. Auch eine mündliche Anfrage von drei Abgeordneten der FDP-Fraktion[1] führte nur zu einer Mängelauflistung der Landesregierung, nicht jedoch zu deren Behebung. Als offene Mängel wurden benannt:

1. Die Aussagen zur Risikoanalyse sind weiterhin unvollständig.
2. Die erforderliche Mandantenfähigkeit des Verfahrens im datenschutzrechtlichen Sinn ist nicht erwiesen, das heißt, eine strikt getrennte Datenhaltung zwischen Niedersachsen und Bremen.
3. Das Rechte-Rollenkonzept ist zu vervollständigen.
4. Die Protokollierung ist um fehlende Komponenten und Maßnahmen zu ergänzen.
5. Die Dokumentenlage ist in Teilen lückenhaft, sodass weder der gesicherte und rechtssichere Betrieb noch eine Revisionssicherheit gewährleistet werden können.
6. Aufgrund des festgestellten hohen Schutzbedarfs ist die Verschlüsselung der Inhalts- und der Verkehrsdaten vorzunehmen.
7. Die Fernwartung ist nur mit besonderen, der Schutzstufe „sehr hoch“ angemessenen Sicherheitsmaßnahmen zulässig.

Mängel können nicht mehr beseitigt werden

Ferner teilte die Landesregierung in der Antwort zur mündlichen Anfrage mit, dass wegen der Kündigung des Dienstleisters im Mai 2015 zahlreiche Mängel nicht mehr behoben werden können. Dies betrifft insbesondere die Mängel bei der Mandantentrennung, der Protokollierung sowie der Verschlüsselung der Inhalts- und Verkehrsdaten.

1 Siehe LT-Drs. 17/4865, S. 83-87, Mündliche Anfrage Nr. 56 „Datenschutz in der Praxis der polizeilichen Telekommunikationsüberwachung.“

Zuletzt habe ich den Innenminister im September 2017 schriftlich auf die gravierende Mängellage hingewiesen. Eine Antwort drauf steht noch aus. Zwar konnte das Innenministerium den Vertrag mit dem Dienstleister befristet verlängern, jedoch nur bis Ende 2020. Diese Vertragsverlängerung sorgt aber nicht dafür, dass die Mängel beseitigt werden, sondern stellt lediglich sicher, dass die TKÜ-Anlage wenigstens für eine Übergangszeit gewartet wird.

Betrieb ist rechtswidrig

Festzuhalten bleibt, dass es der verantwortlichen Stelle, dem LKA Niedersachsen, und der Fachaufsichtsbehörde, dem Ministerium für Inneres und Sport, trotz zahlreicher Gespräche und Ankündigungen zum Ende des Berichtszeitraums nicht gelungen ist, die umfangreiche Mängelliste auch nur ansatzweise abzuarbeiten. Von den insgesamt 44 festgestellten Mängeln[2] werden sich nach einer nochmaligen Prüfung durch meine Behörde und nach Abstimmung mit dem LKA Niedersachsen 38 nicht mehr beseitigen lassen. Hierzu zählen die besonders schwer wiegenden Mängel bei der Mandantentrennung, der unzureichenden Protokollierung und der mangelhaften Verschlüsselung der Inhalts- und Verkehrsdaten. Dies führt dazu, dass der Betrieb der TKÜ-Anlage nach wie vor aus Sicht des Datenschutzes rechtswidrig ist.

## Ausweg: RDZ-TKÜ der Küstenländer?

Gemeinsame Anlage von fünf Ländern

Seit 2011 laufen Planungen für ein Kooperationsprojekt „Rechen- und Dienstleistungszentrum Telekommunikationsüberwachung der Polizei im Verbund der norddeutschen Küstenländer (RDZ-TKÜ)". Zum Projekt „RDZ-TKÜ" habe ich mich daher bereits in drei Tätigkeitsberichten ausführlich geäußert. Die beteiligten Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein wollen auf der Grundlage eines Staatsvertrages gemeinsam eine Anlage zur Telekommunikationsüberwachung betreiben, die mittelfristig die bestehenden und technisch überholten TKÜ-Anlagen ersetzen soll. Dies betrifft auch die laufende TKÜ-Anlage des LKA Niedersachsen, die Telekommunikationsvorgänge zur Strafverfolgung und Gefahrenabwehr für niedersächsische und bremische Behörden überwachen kann.

Austausch mit anderen LfD

Auch im Berichtszeitraum wurde das Thema „RDZ-TKÜ" wiederholt auf Fachebene der Rechts- und Technikreferate der Datenschutzbeauftragten der beteiligten Bundesländer erörtert. Dies besonders vor dem Hintergrund der Erfahrungen mit der laufenden Anlage des LKA Niedersachsen und der dort festgestellten erheblichen datenschutzrechtlichen Mängel. Es besteht Einigkeit mit den vier anderen Aufsichtsbehörden, dass Erfahrungen mit dem Hersteller und Dienstleister der TKÜ-Software für diese Anlage erhebliche Auswirkungen auf künftige Ausschreibungen und Leistungsbeschreibungen für das „RDZ-TKÜ" haben müssen. Dies gilt umso mehr, als grundlegende Mängel oder Schwachstellen eine flächendeckende Wirkung auf Betroffene in fünf Bundesländern haben würden.

2 Siehe dazu im Einzelnen 22. Tätigkeitsbericht für die Jahre 2013-2014, S. 28-29.

## Aktueller Stand des Projekts

Staatsvertrag in allen Ländern ratifiziert

Die fünf norddeutschen Länden haben zwischenzeitlich einen Staatsvertrag zur Durchführung des Projekts unterzeichnet. Der Vertrag wurde im Laufe des Jahres 2016 in allen fünf Ländern durch entsprechende Landesgesetze ratifiziert. Änderungswünsche der Datenschutzbehörden wurden übernommen, so z. B. eine Regelung zur Aufsicht über das RDZ-TKÜ. So können datenschutzrechtliche Mängel, die bei einer Prüfung durch eine Aufsichtsbehörde festgestellt werden, wirksam beseitigt werden. Auch stellt der Staatsvertrag sicher, dass die Datenschutzbehörden bei allen Fragen und Entscheidungen zum Datenschutz und zur Datensicherheit eng eingebunden werden.

Anforderungen an Dienstleister

In den vergangenen beiden Jahren fanden zahlreiche Besprechungen der fünf Datenschutzbehörden in beratender Funktion mit dem LKA Niedersachsen als projektverantwortlicher Stelle statt. Hintergrund war die Erstellung der Unterlagen zur Durchführung des Vergabeverfahrens, um einen Dienstleister für den Betrieb und die Systemtechnik des RDZ-TKÜ zu finden. Hierbei ging es im Wesentlichen um die Frage, welche datenschutzrechtlichen Anforderungen an eine Datenverarbeitung im Auftrag bei TKÜ-Maßnahmen zu stellen sind. Die Datenschutzbehörden empfehlen u. a., den Zugriff des Dienstleisters in seiner Funktion als Auftragsverarbeiter auf personenbezogene Daten weitgehend zu vermeiden. Prinzipiell sollte die Anlage vor Ort gewartet werden, denn eine Fernwartung birgt besondere Risiken für einen unberechtigten Zugriff Dritter auf die hochsensiblen Daten.

Ferner bestand Einigkeit, dass die vorhandenen Mängel bei der laufenden TKÜ-Anlage Niedersachsen/Bremen unbedingt zu vermeiden sind. Die neue RDZ-TKÜ-Anlage muss die Anforderungen an eine Mandantenfähigkeit bei der Datenhaltung ebenso erfüllen wie eine ausreichend sichere Verschlüsselungstechnik bei der Datenverarbeitung.

# 3.2 Gravierende Mängel bei Polizei-Messenger NIMes

Der Niedersachsen Messenger (NIMes) soll die Kommunikation der Polizei im Einsatz erleichtern. Diese dienstliche Alternative zu kommerziellen Anbietern begrüße ich sehr, doch noch weist NIMes einige Mängel auf. Nun sind zunächst die Ergebnisse des Pilotbetriebs abzuwarten.

Am 3. Mai 2018 startete das Ministerium für Inneres und Sport das Pilotprojekt NIMes für die niedersächsische Landespolizei. NIMes ist eine sowohl auf Mobiltelefonen wie auch auf stationären Rechnern nutzbare Anwendungssoftware zum sofortigen Nachrichtenversand, dem sogenannten Instant Messaging. Betrieben und gewartet wird das System durch den Landesbetrieb IT.Niedersachsen.

Nur Kommunikationspartner können mitlesen

Der Messenger dient der Kommunikation zwischen zwei oder mehreren Teilnehmern und ermöglicht das Versenden von Text-, Bild-, Video- und Audionachrichten ähnlich den bekannten Messenger-Diensten WhatsApp, Threema oder Telegram. Aus Sicht des Innenministeriums soll die Anwendung eine wichtige Lücke in der Informationssteuerung bei den Einsatzkräften schließen. Ein unberechtigter Zugriff auf die übertragenen Daten soll dabei durch die Ende-zu-Ende-Verschlüsselung vermieden werden. Dies bedeutet, dass nur die unmittelbaren Kommunikationspartner die Nachricht entschlüsseln und den Inhalt lesen können. Das Besondere an dem niedersächsischen Pilotprojekt ist darüber hinaus, dass NIMes auf den privaten Mobiltelefonen der Polizeibeamten installiert wird.

Die Entwicklung einer dienstlichen Alternative zur ungeregelten Nutzung von kommerziellen Messenger-Diensten im Polizeialltag begrüße ich. NIMes weist jedoch gravierende datenschutzrechtliche Mängel auf.

## Sicherheitslücken durch Betrieb auf privaten Handys

Auch in anderen Bundesländern (z. B. Bayern) nutzt die Polizei eigene Anwendungen zur mobilen Kommunikation, stellt dafür aber dienstliche Geräte bereit. In Niedersachsen dagegen sollen die Beschäftigten ihre privaten Endgeräte verwenden. Dieses Konzept des „Bring Your Own Device" integriert die privaten Endgeräte in ein Netz, das dem Austausch dienstlicher und damit besonders schützenswerter Daten dient. Für das Land Niedersachsen bedeutet das eine erhebliche Kostenersparnis. Jedoch entspricht die Einbindung privater Endgeräte nicht der Datensicherheit, die von der Datenschutz-Grundverordnung (DS-GVO) verlangt wird.

Andere Länder nutzen Dienstgeräte

So kann die Polizei nicht gewährleisten, dass auf den privaten Geräten das aktuellste Betriebssystem und veröffentlichte Sicherheitsupdates installiert sind. Diese Updates sorgen u.a. dafür, dass von den Herstellern erkannte Sicherheitslücken in der Anwendung geschlossen werden. Dieser Mangel bei der IT-Sicherheit von NIMes hat unmittelbare Auswirkungen auf den Datenschutz. Es ist nicht auszuschließen, dass über ein nicht aktualisiertes Mobilfunkgerät Unbefugte mittels Schadsoftware wie Trojaner oder Keylogger auf dienstliche Kommunikationsinhalte und damit personenbezogene Daten zugreifen können. Daher fordert meine Behörde den Einsatz dienstlicher Endgeräte, deren Betriebssoftware zentral auf dem jeweils aktuellsten Sicherheitsstandard gehalten wird.

Risiko für IT-Sicherheit

## Ende-zu-Ende-Verschlüsselung verhindert Kontrolle

Ein weiteres Problemfeld ergibt sich aus der Ende-zu-Ende-Verschlüsselung. Auf der einen Seite gewährleistet sie zwar ein Höchstmaß an Sicherheit im Rahmen der Kommunikationswege. Gleichzeitig verhindert sie aber eine unabhängige Datenschutzkontrolle ohne aktives Mitwirken der beteiligten Kommunikationspartner.

Ende-zu-Ende-Verschlüsselungen sind im Rahmen privater Kommunikation das wirksamste Mittel, um ein Höchstmaß an Vertraulichkeit zu gewährleisten. Dienstliche Kommunikation ist jedoch nicht privat angelegt. Vielmehr haben auch der Dienstherr oder Dritte ein Interesse, die Rechtmäßigkeit der Datenverarbeitung in bestimmten Fällen überprüfen zu können. Verfügen jedoch nur die Kommunikationspartner über die Möglichkeit zur Entschlüsselung der Daten, so wie dies bei einer Ende-zu-Ende-Verschlüsselung der Fall ist, dann ist eine datenschutzrechtliche Kontrolle nur noch eingeschränkt möglich.

Dienstliche Kommunikation muss überprüfbar sein

Das Innenministerium sieht hier die Lösung in verpflichtenden Mitarbeitererklärungen. Die Nutzer von NIMes sagen in dieser Erklärung zu, ihren jeweiligen Entschlüsselungscode für datenschutzrechtliche Kontrollen auszuhändigen. Nach meiner Ansicht sind diese Verpflichtungserklärungen der NIMes-Anwender spätestens dann wertlos, wenn es darum geht, disziplinarrechtlichen oder strafrechtlichen Verstößen nachzugehen, da ein Beschuldigter nicht verpflichtet ist, sich selbst zu belasten. Daher habe ich vorgeschlagen, die Ende-zu-Ende-Verschlüsselung bei NIMes so zu verändern, dass neben den Kommunikationsteilnehmern eine dritte unabhängige Person in Kontrollfällen Zugriff auf die Datenverarbeitungsvorgänge hat. Dies wurde vom Innenministerium bisher jedoch abgelehnt.

Mitarbeitererklärung nicht ausreichend

Letztendlich habe ich mich mit dem Innenminister darauf verständigt, die Ergebnisse des Pilotversuchs abzuwarten. Für die dann anstehende Bewertung von NIMes habe ich dem Innenministerium Kriterien für die notwendige Evaluierung vorgeschlagen. Im nächsten Tätigkeitsbericht werde ich auf die weitere Entwicklung eingehen.

# 3.3 Akkreditierungsentzug zum G20-Gipfel

Kurz vor dem G20-Gipfel 2017 in Hamburg wurden Journalisten ihre Akkreditierungen entzogen. Zum Teil basierte diese Entscheidung auf rechtswidrigen Datenverarbeitungen der Polizei,

Über 4800 Journalisten nehmen teil

Im Juli 2017 fand in Hamburg das Treffen der Gruppe der 20 wichtigsten Industrie- und Schwellenländer statt, der sogenannte G20 Gipfel. Das große Medieninteresse spiegelte sich in der Teilnahme von mehr als 4800 Journalisten wieder. Die Medienvertreter mussten im Vorfeld ein Akkreditierungsverfahren durchlaufen, das vom Presse- und Informationsamt der Bundesregierung unter Mitwirkung des Bundeskriminalamtes durchgeführt wurde.

Entzug von 32 Akkreditierungen

Die umfangreichen Überprüfungen im Rahmen des Verfahrens führten dazu, dass insgesamt 32 Journalisten unmittelbar vor der Veranstaltung die bereits erteilte Akkreditierung wieder entzogen wurden. Damit war ihnen der Zugang zum Medienzentrum verwehrt. Sicherheitskreise begründeten dies mit einer Verschärfung der Gefahrenlage für die beteiligten Regierungsvertreter. Eine Neubewertung der vorhandenen polizeilichen Erkenntnisse über einzelne Journalisten habe zum Ausschluss geführt.

## Bundesweite Prüfung der polizeilichen Datenverarbeitung

Schon während und besonders nach dem Gipfel traf die Entziehung der Akkreditierung auf ein erhebliches Medienecho. Daraufhin initiierte die Bundesbeauftragte für den Datenschutz eine bundesweite Überprüfung der polizeilichen Datenverarbeitung anlässlich des G20-Gipfels und bat die jeweiligen Landesbeauftragten für den Datenschutz um Mitarbeit.

Drei Prüffälle in Niedersachsen

Niedersachsen hatte die Rechtmäßigkeit der polizeilichen Datenverarbeitung bei drei der 32 betroffenen Journalisten zu überprüfen. Hierzu wurden durch meine Mitarbeiter die betroffenen Polizeidienststellen aufgesucht, um vor Ort Einblick in die Datenverarbeitungsprozesse zu nehmen. Wesentliche Prüfkriterien waren die Rechtsgrundlage der Speicherung, die Dokumentation und die Speicherdauer.

## Verarbeitung in Teilen rechtswidrig

Im Ergebnis stellte ich fest, dass Teile der Datenverarbeitung bei einem der drei Journalisten rechtswidrig waren, sowohl bei der Polizeidirektion Hannover als auch beim Landeskriminalamt. Der wesentliche Mangel bestand in einer fehlenden Dokumentation der sog. Prognoseentscheidung. Diese spielt bei der Speicherung personenbezogener Daten in polizeilichen Datenbanken eine zentrale Rolle. Die Polizei darf nämlich Daten, die im Rahmen einer Straf-

verfolgungsmaßnahme gewonnen wurden, nur dann zum Zweck der Verhütung von Straftaten speichern, wenn dies wegen der Art, Ausführung oder Schwere der Tat sowie der Persönlichkeit der tatverdächtigen Person zur Verhütung von vergleichbaren künftigen Straftaten dieser Person erforderlich ist. Ferner ist bei einer Speicherung der Daten auch der Zeitraum der Speicherung genau zu bestimmen.

## Verfahren werden überarbeitet

Daten müssen gelöscht werden

Für die genannten Behörden hatte das negative Prüfergebnis verschiedene Konsequenzen. Sofern der Betroffene dem zustimmte, mussten seine Daten gelöscht werden. Ferner wurden das Verfahren zur Dokumentation der Prognoseentscheidung sowie die Einhaltung gesetzlicher Prüffristen überarbeitet. Aufgrund der Mitwirkung der betroffenen Polizeidienststellen und der Aussicht auf ein verbessertes Verfahren verzichtete ich auf eine förmliche Beanstandung.

Die Überprüfung der polizeilichen Datenverarbeitung bei den beiden anderen Journalisten ergab keine Mängel.

# 3.4 Polizei betreibt weiterhin rechtswidrig Bodycams

Die niedersächsische Landespolizei verwendet weiterhin rechtswidrig Körperkameras zur Videoaufzeichnung. Auch nach einer förmlichen Beanstandung durch meine Behörde stützt das Innenministerium den Einsatz der Kameras auf eine nicht ausreichende Rechtsgrundlage. Abhilfe könnte die Neufassung des Polizeigesetzes schaffen.

Einem bundesweiten Trend folgend, beabsichtigte auch die niedersächsische Landespolizei den Einsatz von am Körper getragenen Kameras, Bodycams. Zunächst bestand Einigkeit darüber, dass für den Einsatz der Kameras das Polizeigesetz geändert werden müsse. Diese Auffassung vertrat noch Ende November 2016 der niedersächsische Innenminister auf der Innenministerkonferenz. Für meine Behörde völlig überraschend verkündete der Innenminister jedoch am 12. Dezember 2016 den Start eines Pilotprojekts zur landesweiten Erprobung der Bodycams.

Start des Pilotprojekts

Vom Innenministerium wurde argumentiert, dass aufgrund des technisch eingeschränkten Einsatzes der Kameras die bisherige Gesetzeslage ausreichend sei. Nach Deaktivierung der Pre-Recording-Funktion und der Tonaufzeichnung handele es sich lediglich um offene Bildaufzeichnungen in Kontrollsituationen nach § 32 Abs. 4 Satz 1 des Niedersächsischen Gesetzes über die Sicherheit und Ordnung (Nds. SOG). Dieser Argumentation bin ich nicht gefolgt und habe daher den Einsatz der Bodycams ohne Gesetzesänderung förmlich beanstandet.

Förmliche Beanstandung

Mit der Pre-Recording-Funktion zeichnen die Bodycams kontinuierlich eine bestimmte Zeitspanne (z. B. 30 Sekunden) in einem gesonderten Speicher auf. Diese Aufzeichnungen werden immer wieder mit Ablauf der Zeitspanne überschrieben. Aktiviert ein Polizeibeamter die Aufnahme, wird dann auch die aktuelle Sequenz aus dem Pre-Recording dauerhaft gespeichert und nicht mehr überschrieben.

## Grund für die Beanstandung

Das Gesetz erlaubt es der Polizei zwar, Kameras bei Anhalte- und Kontrollsituationen im Verkehrsraum zur Eigensicherung offen einzusetzen. Diese Regelung hatte aber die Zielrichtung, im Fahrzeug fest installierte Kameras einzusetzen, nicht jedoch am Körper getragene Bodycams. Durch die Mobilität der Körperkameras und das Filmen aus unmittelbarer Nähe zum Betroffenen, wird im Vergleich zu einer fest installierten und damit unbeweglichen Kamera besonders schwerwiegend in die Grundrechte eingegriffen. Durch diese Unmittelbarkeit der Datenerhebung und der fehlenden Möglichkeit sich der Überwachung zu entziehen, wird ein besonders hoher Druck gegenüber den Betroffenen aufgebaut. Ferner entspricht die vom Innenministerium heran-

Schwerwiegender Eingriff in Grundrechte

gezogene Rechtsgrundlage nicht mehr den Anforderungen, die das Bundesverfassungsgericht für eine dem Grundsatz der Bestimmtheit genügende Norm zur Datenverarbeitung aufgestellt hat. Das heißt, aus dem Gesetzeswortlaut muss eindeutig hervorgehen, unter welchen Voraussetzungen Daten verarbeitet werden dürfen. Folgerichtig musste ich wegen des rechtswidrigen Einsatzes der Bodycams eine Beanstandung aussprechen.

## Innenministerium mit Erprobung zufrieden

Innenministerium reicht Vorabkontrolle nach

Die Polizei beendete die Erprobungsphase am 31. März 2017 beendet. Die dabei gesammelten Erkenntnisse trug das Innenministerium in einem Evaluationsbericht zusammen. Im Bericht heißt es, Bodycams seien ein geeignetes Mittel zur Eigensicherung der Polizeibeamten. Diese Feststellung wurde jedoch nicht durch Einzelfälle des Pilotverfahrens belegt. Stattdessen wurde die deeskalierende Wirkung der Körperkameras mit den Ergebnissen aus anderen Ländern begründet, ohne jedoch auf die zitierten Länderstudien näher einzugehen. Das Innenministerium hatte das hauptsächliche Augenmerk der Erprobungsphase auf die Praktikabilität der Kameras im alltäglichen Einsatz gelegt. Da dieser Aspekt eine datenschutzrechtlich geringe Rolle spielt, hielt ich meine Beanstandung weiterhin aufrecht.

Im Ausschuss für Inneres und Sport des niedersächsischen Landtags bekam ich am 16. März 2017 Gelegenheit zur Stellungnahme. Ich stellte hier ausdrücklich noch einmal fest, dass der § 32 Abs. 4 Nds. SOG nicht die Anforderung an die Bestimmtheit und Normenklarheit einer Eingriffsnorm erfüllt. Vielmehr muss der Gesetzgeber eine spezielle Rechtsgrundlage für Bodycams schaffen und damit entscheiden, ob und in welchem Umfang Kameras im Polizeialltag eingesetzt werden. Auch wiederholte ich noch einmal meine Forderung, eine vom Gesetz vorgeschriebene Vorabkontrolle zu erstellen, um die mit dem Einsatz der Bodycams verbundenen Risiken für die Betroffenen zu minimieren. Diese wurde zwischenzeitlich vom Innenministerium nachgereicht. Die Vorabkontrolle hätte jedoch vor dem Beginn des Pilotverfahrens erstellt werden müssen.

## Ausbau trotz weiter fehlender Rechtsgrundlage

Im September 2018 schloss das Landespolizeipräsidium mit einem Anbieter einen Vertrag über den Erwerb von 500 Kameras, die innerhalb der nächsten fünf Jahre angeschafft werden sollen. Es ist für mich nicht nachvollziehbar, dass die Landesregierung vollendete Tatsachen schuf, obwohl zu dieser Zeit die Gesetzesberatungen zum neuen Polizei- und Ordnungsbehördengesetz noch liefen. Auch wurde die Zusicherung des Innenministeriums, nach meiner Beanstandung das weitere Vorgehen mit meiner Behörde eng abzustimmen, nicht eingehalten.

Keine Abstimmung mit meiner Behörde

Dieses Beispiel macht besonders deutlich, dass der Datenschutz sehr häufig eine nur untergeordnete Rolle spielt, wenn Fragen der inneren Sicherheit politisch im Vordergrund stehen. Dies ist aus meiner Sicht nicht hinnehmbar, denn Freiheit und Sicherheit schließen sich nicht gegenseitig aus, sondern müssen in Einklang gebracht werden. So kann der Einsatz von Bodycams durchaus verfassungs- und damit datenschutzkonform geregelt werden. Dies ist jedoch allein Aufgabe des Gesetzgebers und nicht der Ministerialverwaltung. Demzufolge begrüße ich es ausdrücklich, dass mit dem neuen Polizei- und Ordnungsbehördengesetz eine spezielle Rechtsgrundlage im Nachgang geschaffen wird, die den Einsatz von Bodycams bei der Polizei präzise regelt.

Rechtsgrundlage im neuen Polizeigesetz

# 3.5 Polizei-Leitstellen erfüllten gesetzliche Vorgaben nicht

Leitstellen der Polizei verarbeiten hochsensible Daten, deren unsachgemäße Handhabung Gesundheit, Freiheit oder sogar das Leben des Betroffenen beeinträchtigen kann. Umso schlimmer ist es, dass sich die Leitstellen über Jahre nicht an die datenschutzrechtlichen Vorgaben hielten. Inzwischen ist allerdings Besserung in Sicht.

Bereits 2005 gab es erste Planungen der damaligen Landesregierung kooperative Leitstellen in Niedersachsen zu errichten. Neben einer Reduzierung der Leitstellen sollten durch die Einrichtung von sogenannten „bunten" Leitstellen Polizei, Feuerwehr und Rettungsdienste unter einem Dach zusammengefasst werden. Unter Wahrung der jeweiligen Selbstständigkeit der verschiedenen Träger war beabsichtigt, eine einheitliche Technik und gemeinsame Gebäude zu nutzen.

## Fünf kooperative Leitstellen in Niedersachsen

Inzwischen gibt es niedersachsenweit fünf kooperative Regionalleitstellen in Osnabrück, Hameln, Oldenburg, Lüneburg und Wittmund. In anderen Teilen des Landes, wie in Göttingen und Hannover, betreibt die Polizei ihre Leitstellen weiterhin eigenständig. Für alle Leitstellen gilt, dass sie hochsensible personenbezogene Daten verarbeiten, deren unsachgemäße Handhabung im Einzelfall Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnten. Auch das Ansehen oder die Existenz des Betroffenen könnten bedroht sein. Die unsachgemäße Handhabung umfasst nicht nur den vorsätzlichen Missbrauch, sondern auch unzureichenden Schutz vor menschlichen Fehlern, organisatorischen Mängeln, technischem Versagen und höherer Gewalt.

Verarbeitung sensibler Daten nur mit Datenschutzfolgenabschätzung

Diesen Gefahren für die Rechte der Betroffenen begegnet der Gesetzgeber mit unterschiedlichen datenschutzrechtlichen Bestimmungen. So wurde unter anderem für Daten, deren Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, bislang eine Vorabkontrolle gefordert. Nach dem neuen Recht der DS-GVO tritt an ihre Stelle seit dem 25. Mai 2018 die Datenschutzfolgenabschätzung.

Mit der Vorabkontrolle bzw. der Datenschutzfolgenabschätzung wird die Beherrschbarkeit neuer Informations- und Kommunikationsverfahren vor deren Einführung überprüft. Es werden die Abläufe der automatisierten Datenverarbeitung transparent gemacht, Gefahren für die Rechte der betroffenen Bürgerinnen und Bürger aufgezeigt, Risiken abgeschätzt und Sicherungskonzepte entworfen. Die Methodik ist auch dafür geeignet, Lösungen für einen datenschutzgerechten Technikeinsatz zu finden.

## Muster-Vorabkontrolle mangelhaft

Die Polizeidirektion Oldenburg war mit einer Muster-Vorabkontrolle für die Kooperative Großleitstelle Oldenburg beauftragt, die sie 2012 fertig stellte. Die Vorabkontrolle wies jedoch einen erheblichen Mangel auf: Die Risiken wurden zwar wie gefordert ausführlich beschrieben, es fehlte jedoch an der Festlegung der technisch-organisatorischen Schutzmaßnahmen, um diesen Risiken zu begegnen. Trotz mehrfachen Aufforderung durch meine Behörde über die Folgejahre gelang es der Polizeidirektion Oldenburg nicht, die Vorabkontrolle zufriedenstellend zu beenden und als Muster für andere Leitstellen zur Verfügung zu stellen.

Maßnahmen zur Risikobewältigung fehlen

Als technische Maßnahmen sind physisch umsetzbare Handlungen wie beispielsweise der Einsatz einer Firewall zu verstehen. Zu den organisatorischen Maßnahmen zählt unter anderem das Verfassen von Handlungsanweisungen.

Somit liegt mir bis zum Zeitpunkt dieses Berichts keine den gesetzlichen Anforderungen entsprechende Vorabkontrolle bzw. inzwischen Datenschutzfolgenabschätzung vor. Die nachvollziehbare Feststellung, dass durch entsprechende technisch-organisatorische Maßnahmen sensible personenbezogene Daten ausreichend geschützt sind, bleibt die Polizei bis heute schuldig. Diesen rechtswidrigen Zustand habe ich mehrfach gegenüber dem Innenministerium gerügt.

Mehrfache Rüge

## Keine gesetzeskonforme Auftragsverarbeitung

Bei der überwiegenden Anzahl der Leitstellen wird die Einsatzleit-Software durch beauftragte IT-Unternehmen gewartet. Diese führen regelmäßig auch Fernwartungen durch und greifen so von außen auf die Datenverarbeitungssysteme zu. In diesem Zusammenhang habe ich festgestellt, dass die Dienstleistung der Fernwartung datenschutzrechtlich nicht ausreichend durch Verträge zur Auftragsverarbeitung abgesichert wurde. Verträge waren entweder nicht vorhanden oder unzureichend.

Allgemeine Wartungsverträge nicht ausreichend

So müssen beispielsweise die Verschlüsselung der Leitung, die Zugriffsrechte, der Umfang und die Protokollierung des Zugriffs zwischen Auftraggeber und -nehmer geregelt werden. Die Polizeidirektionen konnten bislang nur allgemein gehaltene Support- und Wartungsverträge vorlegen, die keine detaillierte Regelung des Fernzugriffs aufwiesen. Diesen eindeutig rechtswidrigen Zustand habe ich ebenfalls gegenüber dem Innenministerium gerügt.

## Kurskorrektur der Polizeidirektionen erkennbar

Nach meinem 2018 geführten Dialog mit dem Innenministerium ist ein Problembewusstsein für die Beseitigung der bestehenden datenschutzrechtlichen Mängel bei den Leitstellen in Niedersachsen entstanden.

Ende 2018 hielt die Polizei einen Workshop zur Vereinheitlichung der Prüf- und Löschfristen sowie zu Recherchemöglichkeiten in den Datenbanken der Leitstellen ab. Beteiligt waren alle

Einheitliche Kriterien für Datenverarbeitung

Polizeidirektionen, die eine Leitstelle betreiben. Die Polizei legte dabei einheitliche Kriterien für die Datenverarbeitung in Leitstellen fest, die per Erlass des Innenministeriums für verbindlich erklärt wurden. Meine Prüfung ergab, dass sich das Ergebnis an datenschutzrechtlichen Vorgaben orientierte und keine weitere Kritik meinerseits erforderte.

Im Hinblick auf die fehlende Datenschutzfolgenabschätzung sicherte das Innenministerium mir eine Fertigstellung im Jahr 2019 zu. Der Aspekt der Fernwartung im Zusammenhang mit der Auftragsverarbeitung bleibt derzeit in den Polizeidirektionen Hannover, Lüneburg und Göttingen ungeregelt. Hier erwarte ich zeitnahe Nachbesserungen.

Ich werde auch im Jahr 2019 ein Hauptaugenmerk auf die Verarbeitung personenbezogener Daten in den Leitstellen der Polizei werfen und dafür sorgen, möglichst zeitnah eine rechtskonforme Verarbeitung in allen Bereichen herzustellen.

# 3.6 Polizei speichert rechtswidrig Daten von friedlichen Demonstranten

Die Polizei speicherte die Daten hunderter Demonstrationsteilnehmer teilweise für mehrere Jahre nach dem Veranstaltungsende. Das steht klar im Widerspruch zum Niedersächsischen Versammlungsgesetz. Inzwischen ist diese rechtswidrige Praxis beendet – durch Nachfragen aus der Politik und den beharrlichen Einsatz meiner Behörde.

## Bürgereingabe löst umfassende Prüfung aus

Auslöser für eine umfassende datenschutzrechtliche Prüfung war eine Eingabe aus dem Jahr 2015. Der Betroffene hatte nach Anmeldung und Durchführung einer friedlich verlaufenen Versammlung angefragt, welche seiner personenbezogenen Daten durch die Polizei gespeichert worden waren. Nachdem er dort keine ausreichende Auskunft erhalten hatte, wandte er sich an meine Behörde. Ich musste feststellen, dass er ohne Rechtsgrundlage weiter im Zusammenhang mit der Versammlung im polizeilichen Vorgangssystem NIVADIS gespeichert war.

Polizei gibt nicht ausreichend Auskunft

## Verletzung des Grundrechts auf Versammlungsfreiheit

Die Datenverarbeitung anlässlich von Versammlungen greift in das Grundrecht auf informationelle Selbstbestimmung ein, wie auch in das Grundrecht der Versammlungsfreiheit. Laut Bundesverfassungsgericht darf der Bürger darauf vertrauen, dass er sein Grundrecht auf Versammlungsfreiheit frei, offen, nicht reglementiert und grundsätzlich „staatsfern“ ausüben kann. Eingeschränkt wird das Grundrecht u.a. durch die Regelungen des Niedersächsischen Versammlungsgesetzes.

Neben der Rechtsgrundlage für die Datenerhebung über den Verantwortlichen einer Versammlung finden sich im Gesetz auch die Regelungen zur weiteren Datenverarbeitung. Die im Zusammenhang mit der Anmeldung einer Versammlung verarbeiteten personenbezogenen Daten müssen unverzüglich nach deren Ende gelöscht werden. Ausnahme: Die Daten werden zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt.

Daten müssen nach Demo-Ende gelöscht werden

## Recherche bei Polizei liefert erschreckendes Ergebnis

Im beschriebenen Fall standen weder die Verfolgung einer Straftat noch einer Ordnungswidrigkeit im Raum. Es war also rechtswidrig, die personenbezogenen Daten des Versammlungsteilnehmers weiter in einer polizeilichen Da-

tenbank zu speichern. Um festzustellen, ob es sich um einen Einzelfall oder um einen systematischen Fehler handelte, veranlasste ich für die Jahre 2003 bis 2015 eine niedersachsenweite Recherche im polizeilichen Vorgangsbearbeitungssystem. Ich wollte wissen, ob es weitere Fälle gab und falls ja, wie oft personenbezogene Daten nach dem Ende einer friedlichen Versammlung nicht unverzüglich gelöscht worden waren.

Überprüfung in ganz Niedersachsen

Zu meinem Erschrecken handelte es sich um hunderte Fälle, in denen die Polizei die Daten von friedlichen Versammlungsteilnehmern jahrelang recherchierbar gespeichert hatte. Sämtliche niedersächsischen Polizeidirektionen waren betroffen. In insgesamt 512 Einzelfällen waren personenbezogene Daten zum Zeitpunkt meiner Erhebung noch gespeichert.

## PD Lüneburg widerspricht als einzige

Ich forderte die einzelnen Polizeidirektionen (PD) zu Stellungnahmen auf. Sie sollten überprüfen, inwieweit die Datenspeicherung in den 512 ermittelten Einzelfällen rechtmäßig war. Nur in einem einzigen Fall konnte nachgewiesen werden, dass die Datenspeicherung auf der Grundlage des geltenden Rechts zulässig und auch weiterhin erforderlich ist. Die übrigen 511 Datensätze wurden aus dem polizeilichen Vorgangsbearbeitungssystem unverzüglich gelöscht. Damit konnte meine Behörde einen ersten schnellen Erfolg verbuchen.

Nur eine Speicherung zulässig

Einzig die PD Lüneburg widersprach meiner Rechtsauffassung und gab an auch weiterhin die personenbezogenen Daten über das Versammlungsende hinaus zur Dokumentation des Einsatzgeschehens zu speichern. Im Dezember 2016 unterrichtete ich den Innenausschuss des Niedersächsischen Landtags über diese rechtswidrige Verfahrensweise, woraus eine „Kleine Anfrage" der FDP-Fraktion an die Landesregierung resultierte. Die Landesregierung antwortete, dass man die PD Lüneburg noch einmal auf die Rechtslage hingewiesen habe. Sie möge daher ihre Rechtsauffassung noch einmal kritisch hinterfragen.

## Erfolg für den Datenschutz

Im Lauf des Jahres 2017 teilte die PD Lüneburg schließlich meiner Behörde mit, dass man nun alle personenbezogenen Daten, insgesamt 135 Vorgangsnummern, gelöscht habe.

Damit konnte ein mehrjähriges Prüfverfahren erfolgreich abgeschlossen werden. Ein datenschutzrechtlich engagierter Bürger hat durch seine Eingabe nicht nur die Löschung seiner rechtswidrig gespeicherten Daten bei der Polizei erreicht. Er deckte darüber hinaus einen weit verbreiteten datenschutzrechtlichen Missstand auf, der von meiner Behörde mit Unterstützung des Landtages abgestellt werden konnte.

In angemessener Zeit werde ich eine erneute stichpunktartige Prüfung veranlassen, um festzustellen, ob die Polizeibehörden inzwischen ihren Löschverpflichtungen nachkommen.

# 3.7 Pilotprojekt „Section Control“ gestartet, aber ohne ausreichende Rechtsgrundlage

Seit dem 19. Dezember 2018 wird im Rahmen einer Erprobungsphase auf einer Strecke von 2,2 Kilometer auf der B 6 zwischen den Ortschaften Laatzen und Gleidingen die Geschwindigkeit von Kraftfahrzeugen überwacht. Grundlegende Neuerung des Verfahrens ist es, dass keine, wie bisher praktizierte, punktuelle Überwachung der Geschwindigkeit erfolgt, sondern die Durchschnittsgeschwindigkeit innerhalb eines festgelegten Streckenabschnitts (Section Control) ermittelt wird. Durchfährt das Fahrzeug den Streckenabschnitt zu schnell soll nach Ablauf einer vierwöchigen Testphase ein Bußgeld verhängt werden.

Trotz fehlender Rechtsgrundlage hat das Ministerium für Inneres und Sport den auf 18 Monate angelegten Pilotzeitraum gestartet. Nach einer neueren Entscheidung des Bundesverfassungsgerichts im Dezember 2018 hat meine Behörde das Ministerium aufgefordert, den Betrieb solange auszusetzen, bis der Gesetzgeber eine ausreichend bestimmt gefasste Rechtsgrundlage geschaffen hat, die die Eingriffe in die Grundrechte der Fahrzeugführer legitimiert.

## Wie funktioniert „Section Control“?


Nach Angaben des Herstellers wird die Überschreitung der Durchschnittsgeschwindigkeit in Teilschritten ermittelt:

Jeweils am Ein- und Ausfahrtsquerschnitt der Anlage werden die Fahrzeuge detektiert, klassifiziert und durch Kameras fotografisch von hinten erfasst. Sogleich nach Erfassung des Fahrzeugkennzeichens sowie weiterer personenbezogener Angaben (Fahrtrichtung, Ort und Zeit) werden diese Daten hochverschlüsselt, indem ein sog. Hashwert gebildet wird. Dies ist eine anhand einer mathematischen Funktion gebildete Zeichenfolge, die eine manuelle Rückführbarkeit auf das amtliche Kennzeichen sowie auf die weiteren Daten ausschließt. Nach dem Durchfahren des Einfahrtquerschnitts (1. Kamera) und des Ausfahrtsquerschnitts (2. Kamera) erhält ein Auswerterechner die entsprechenden Hashwerte des durchfahrenden Fahrzeugs und ermittelt anhand der eingestellten Wegstreckenlänge die Durchfahrtzeit und damit die gefahrene Durchschnittsgeschwindigkeit. Wird ein Verstoß festgestellt, so fertigt eine dritte Kamera wie bei den bekannten „Blitzern“ eine Frontaufnahme vom Fahrzeug und seinem Fahrzeugführer, um ein Bußgeld verhängen zu können. In allen anderen Fällen werden die Daten sofort und unwiederbringlich gelöscht.

## Rechtslage bis zum Dezember 2018

In seinem Urteil vom 11.03.2008[1] zum Einsatz von Kennzeichenlesegeräten hat das Bundesverfassungsgericht ausgeführt, dass ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung nicht vorliegt, wenn das von der Technik erfasste Fahrzeugkennzeichen unverzüglich mit dem Fahndungsbestand der Polizei abgeglichen und ohne weitere Auswertung sofort wieder gelöscht wird, sog. Nichttrefferfall. Diese Fallkonstellation tritt bei Section Control bei der überwiegenden Anzahl von Fahrzeugen auf, die sich an die Geschwindigkeit halten. Das Gericht hat jedoch im selben Urteil eine ausdrückliche Rechtsgrundlage für die Fälle gefordert, bei denen ein Abgleich des Fahrzeugkennzeichens mit der Fahndungsdatei zu einem Treffer führt und sich dementsprechend weitere polizeiliche Maßnahmen anschließen. In diesen Trefferfällen findet zweifelsfrei eine Datenverarbeitung und damit ein Grundrechtseingriff statt. Übertragen auf Section Control sind das die wenigen Fälle, bei denen die dritte Blitzerkamera ausgelöst wird, weil ein Geschwindigkeitsverstoß anzunehmen ist.

Auf der Grundlage dieses Urteils des Bundesverfassungsgerichts aus dem Jahr 2008 hat mein Vorgänger im Amt im August 2015 gegen die vom Innenministerium beabsichtigte Erprobung von Section Control für die Dauer von 18 Monaten keine Einwände erhoben. Damit waren jedoch einige Bedingungen verbunden, so z. B. dass die Anlage Daten nur zur Geschwindigkeitsmessung verarbeitet und dass bei Nichttrefferfällen sämtliche Daten sofort und spurenlos zu löschen sind. Auch muss der Autofahrer bei Einfahrt in die Anlage durch ein deutlich sichtbares Schild auf die Geschwindigkeitsmessung aufmerksam gemacht werden.

## Umfassende technische Prüfungen

Die Polizeidirektion Hannover erstellte als verantwortliche Stelle im Herbst 2015 für das Projekt „Section Control" eine Vorabkontrolle und eine Verfahrensbeschreibung, um insbesondere einen Datenmissbrauch durch einen unberechtigten Zugriff weitgehend auszuschließen. Sämtliche Unterlagen wurden von meiner Behörde eingehend datenschutzrechtlich geprüft. Hierzu fanden mit der Polizei und dem Hersteller der Anlage Ende 2015 mehrere Besprechungen statt. Im Ergebnis wurden festgestellte Mängel beim technisch-organisatorischen Datenschutz aufgrund meiner Hinweise weitestgehend abgestellt. Der Hersteller und die Polizei haben zugesagt, noch vorhandene Mängel während des Pilotbetriebs zeitnah zu beseitigen. Unter anderem hat der Hersteller angekündigt, die eingesetzte Technik zur Verschlüsselung der Daten weiter zu optimieren. Meine Behörde wird daher nach Abschluss des Pilotverfahrens den technisch-organisatorischen Datenschutz bei der Section-Control-Anlage nochmals einer umfassenden Prüfung unterziehen. Im Mai 2016 wurde der Pilotbetrieb von mir datenschutzrechtlich frei gegeben. Anschließend fanden umfassende Prüfungen der Physikalisch-Technischen-Bundesanstalt statt, die erst in 2018 abgeschlossen wurden.

1 1 BvR 2074/05 und 1 BvR 1254/07; NJW 2008, 1505

## Bundesverfassungsgericht ändert seine Rechtsprechung

Im Dezember 2018 hatte sich das Bundesverfassungsgericht in zwei Beschlüssen erneut mit der Datenverarbeitung beim Einsatz von Kennzeichenlesegeräten befasst.[2] In diesen Beschlüssen zur Frage der Verfassungsmäßigkeit der Regelungen in Bayern, Hessen und Baden-Württemberg ändert das Gericht seine Rechtsansicht und stufte auch die Fälle der sog. Nichttreffer als Grundrechtseingriff ein. Ein Eingriff in das Grundrecht der informationellen Selbstbestimmung liege auch dann vor, wenn bei einer systematischen Überwachungsmaßnahme ein Fahrzeugkennzeichen erfasst und im Nichttrefferfall die Daten sofort wieder spurenlos gelöscht werden. Im Ergebnis bedeutet diese Abkehr von der Rechtsprechung aus dem Jahr 2008, dass bei Section Control ein Grundrechtseingriff und damit eine Datenverarbeitung bei allen Fahrzeugen stattfindet, die die Anlage durchfahren, unabhängig davon, ob ein Geschwindigkeitsverstoß vorliegt oder nicht.

Die Kehrtwende des Bundesverfassungsgerichts muss zwangsläufig zu einer rechtlichen Neubewertung von Section Control führen. Es kann nicht außer Acht gelassen werden, dass in die Grundrechte aller Bürgerinnen und Bürger eingegriffen wird, indem Section Control systematisch alle Fahrzeugkennzeichen und weitere personenbezogene Daten erfasst, für einen gewissen Zeitraum speichert und verarbeitet. Das Bundesverfassungsgericht sagt hierzu klar und deutlich, dass eine solche Maßnahme nicht erst hinsichtlich ihrer Folgen, sondern schon als solche freiheitsbeeinträchtigend wirkt.

Täglich fahren bis zu 15.000 Fahrzeuge durch die Anlage. In welchem Ausmaß und zu welchem Zweck in die Grundrechte dieser zunächst unbescholtenen Bürgerinnen und Bürger eingriffen werden darf, hat allein der Gesetzgeber zu entscheiden.

Der Entwurf eines neuen Polizei- und Ordnungsbehördengesetzes enthält eine spezielle Rechtsvorschrift für die Geschwindigkeitskontrolle mittels Section Control.

Auf die weitere Entwicklung der Sach- und Rechtslage werde ich im nächsten Tätigkeitsbericht umfassend eingehen.

2 Beschlüsse vom 18.12.2018, 1 BvR 142/15, 1 BvR 2795/09 und 1 BvR 3187/10

# F.4. Datenschutz in Kommunen und Landesverwaltung

## 4.1 Umstellung auf neue Datenschutzregelungen im Kommunalbereich

Mit einer Prüfung bei 150 Gemeinden, Städten und Landkreisen sollte Ende 2018 der Sachstand der notwendigen Anpassungsarbeiten zur Umsetzung der Anforderungen der bereits im Jahre 2016 In-Kraft-getretenen und seit dem 25. Mai 2018 unmittelbar geltenden DS-GVO festgestellt werden.

Mit der Abfrage wollte ich in Erfahrung bringen, vor welchen Problemen die Kommunen bei der Umsetzung der DS-GVO stehen. Im Zentrum der Prüfung standen Fragen wie:

Sachstand und Probleme in Erfahrung bringen

- Welche Anforderungen der DS-GVO konnten die Verantwortlichen bereits in vollem Umfang umsetzen?
- Bei welchen Themen gibt es noch Probleme?
- Zu welchen Einzelaspekten benötigen die Verantwortlichen weitere Unterstützung?

Darüber hinaus sollte das Bewusstsein der verantwortlichen Stellen für den Datenschutz im Allgemeinen geschärft werden.

Die Auswertung der Stellungnahmen erfolgt zu den Themenfeldern

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

Die genauen Ergebnisse der Prüfung werden in einem Abschlussbericht anonymisiert zusammengefasst und im Frühjahr 2019 veröffentlicht. Ich werde sie in meinem nächsten Tätigkeitsbericht detailliert vorstellen.

# 4.2 Fragen und Beschwerden zum Wahlrecht

Vor den Wahlen zum Deutschen Bundestag und zum Niedersächsischen Landtag erhielt ich vermehrt Eingaben von Bürgern zur Verarbeitung ihrer personenbezogenen Daten. Die ausgewählten Beispiele zeigen jedoch, dass es sich hierbei nur selten um tatsächliche Verstöße gegen den Datenschutz handelt.

Vor einer Wahl werden die Wahlberechtigten durch die Gemeinde mit einer Benachrichtigungskarte darüber informiert, wo und wann sie ihre Stimme abgeben können. Die Vorlage der Karte ist Voraussetzung für die persönliche Wahl oder für den Antrag auf Briefwahl. Die Wahlkarten werden als Postkarte versendet, auf der Vorname, Name und Wohnanschrift stehen.

## Geburtsjahr nur als Ausnahme zulässig

Zur Bundestagswahl 2017 verschickte eine Gemeinde Karten, auf denen zusätzlich das Geburtsjahr des Empfängers aufgedruckt war. Eine pauschale Kennzeichnung der Karten mit dem Geburtsjahr ist jedoch gesetzlich nicht vorgesehen. Das ist nur zulässig, um Wähler gleichen Namens, die dieselbe Anschrift teilen, erreichen zu können. Im vorliegenden Fall handelte es sich um ein Versehen und die betroffene Gemeinde entschuldigte sich in der Tagespresse bei den Bürgern. Zudem habe ich empfohlen, statt des Geburtsjahrs den datenschutzfreundlicheren Zusatz „senior“ und „junior“ zu verwenden.

Senior und Junior statt Geburtsjahr

## Nur erforderliche Daten hinter QR-Codes

Teilweise war auf Wahlbenachrichtigungskarten auch ein QR-Code zur Online-Beantragung von Briefwahlunterlagen aufgedruckt. Der Code leitete zu einem Online-Formular weiter, das neben den auf der Karte aufgedruckten personenbezogenen Daten auch das Geburtsdatum des Wählers anzeigte. Mich erreichte eine Beschwerde, dass unbefugte Dritte den QR-Code auslesen und so an die dahinter liegenden Daten gelangen könnten. Zunächst habe ich festgestellt, dass es nicht erforderlich ist, das Geburtsdatum im QR-Code zu hinterlegen. Was die Möglichkeit des Code-Auslesens im offenen Versand angeht, so gewährleistet das Postgeheimnis, dass unbefugte Dritte keinen Zugriff auf die hinter dem Code liegenden Daten haben.

Postgeheimnis schützt vor Zugriff Dritter

Im vorliegenden Fall handelte es sich um ein Versehen. Die betroffene Gemeinde sagte zu, bei der nächsten Wahl besondere Aufmerksamkeit auf die per QR-Code abrufbaren Daten legen zu wollen.

## Briefwahlunterlagen zur Bundestagswahl

Neben der persönlichen Stimmabgabe im Wahllokal besteht die Möglichkeit, per Briefwahl zu wählen. Nach Beantragung der Briefwahlunterlagen werden diese gemeinsam mit dem Wahlschein entweder per Post versendet oder liegen zur Abholung im Wahlamt bereit. Es besteht zudem die Möglichkeit, Briefwahlunterlagen vor Ort im Wahlamt auszufüllen und dort direkt wieder abzugeben.

Bei der Briefwahl wird der Wahlschein vom Wähler unterschrieben in einen verschlossenen Briefumschlag gegeben. Dieser Umschlag wird zusammen mit einem weiteren verschlossenen Umschlag, der den Stimmzettel enthält, in einen dritten verschlossenen Umschlag (Wahlbrief) gegeben. Dieser wird dann abgeschickt oder im Wahlamt abgegeben.

Bürgerinnen und Bürger äußerten Bedenken, dass durch den Versand aller Unterlagen in einem Umschlag die Stimmabgabe auf dem Stimmzettel den auf dem Wahlschein enthaltenen personenbezogenen Daten (Name, Adresse, Geburtsdatum) zugeordnet werden könnte und so das Wahlgeheimnis gefährdet würde. Auch wurde teilweise die geforderte Abgabe einer eidesstattlichen Versicherung, dass der Stimmzettel vom Wähler persönlich gekennzeichnet wurde, in Frage gestellt. Grund war die Annahme, dass es sich bei der vorzeitigen Stimmangabe im Wahllokal um eine vorgezogene Präsenzwahl handelt und die Erklärung der Versicherung per Unterschrift daher entbehrlich sei.

Sorge um das Wahlgeheimnis

Lassen sich Bürgerinnen und Bürger die Briefwahlunterlagen im Wahlamt aushändigen und wählen direkt vor Ort, handelt es sich jedoch um eine Briefwahl und nicht um eine vorgezogene Präsenzwahl. Gemäß § 66 Bundeswahlordnung werden im Rahmen der Briefwahl die Wahlbriefe im Wahlamt zunächst gesammelt und erst am Wahltag dem zuständigen Briefwahlvorstand übergeben. Dieser öffnet die Wahlbriefe, prüft die Gültigkeit des Wahlscheins und gibt die zugehörigen verschlossenen Stimmzettelumschläge in die Wahlurne. Eine Zuordnung der personenbezogenen Daten zur jeweiligen Stimmabgabe eines Wählers ist somit nicht möglich.

## Repräsentative Statistik mit Wahlgeheimnis vereinbar

Die repräsentative Wahlstatistik gehört zu den wichtigsten Quellen der Wahlforschung. Das Wahlergebnis wird hierbei statistisch ausgewertet, um Aufschluss über das Wahlverhalten verschiedener Bevölkerungsgruppen zu erhalten. Die Wahlzettel, die in die Statistik einfließen, enthalten einen Aufdruck mit Informationen zu Geschlecht und Altersgruppe des Wählers. Mich erreichten einige Beschwerden von Bürgerinnen und Bürgern, die Bedenken zur Vereinbarkeit der aufgedruckten Angaben mit dem Grundsatz der geheimen Wahl hatten.

Stimmzettel mit Information zu Alter und Geschlecht

Voraussetzung für die Verwendung von Stimmzetteln mit Unterscheidungsmerkmalen und die Durchführung einer repräsentativen Wahlstatistik ist, dass der Wahlbezirk mindestens 300 Wahlberechtigte umfasst. So ist gewährleistet, dass jeweils mehrere Frauen und Männer jeder Altersgruppe von der Statistik erfasst werden. Personenbezogene Daten wie Name, Anschrift oder Geburtsdatum werden nicht erfasst, so dass aus den abgegebenen Stimmzetteln keinerlei Rückschlüsse auf eine konkrete Einzelperson gezogen werden können.

# 4.3 Melderechtliche Anfragen und Beschwerden

Gerade im Bereich des Melderechts haben Bürger immer wieder Kontakt zu Behörden. Deshalb erreichten mich dazu auch in diesem Berichtszeitraum wieder zahlreiche Anfragen, von denen ich hier einige beispielhaft darstellen möchte.

## Weitergabe von Meldedaten zur Erfüllung öffentlicher Aufgaben

Mich erreichte die Frage, ob die Meldebehörde Adressdaten immobiler Senioren an die Kommune weitergeben darf. Ziel war es, dass Vertreter der Kommune die Senioren in der Vorweihnachtszeit zu Hause besuchen und beschenken können.

Kommune entscheidet selbst, was öffentliche Aufgabe ist

Die Meldebehörde darf Daten aus dem Melderegister innerhalb der Kommune weitergeben, wenn die Daten zur Erfüllung öffentlicher Aufgaben erforderlich sind. Die Kommune entscheidet in eigener Verantwortung darüber, welche Daten erforderlich sind, damit sie ihre Aufgaben erfüllen kann[1]. Was die Kommune wiederum als Teil der öffentlichen Aufgabe versteht, kann sie Bereich der Selbstverwaltung auch durch Ratsbeschluss oder Satzung festlegen.

## In folgenden Fällen ist dies jedoch nicht zulässig:

Keine Weitergabe für wirtschaftliche Zwecke

- Weitergabe zu wirtschaftlichen Zwecken, da dies zu einem Wettbewerbsvorteil der Kommune führen könnte (z. B. Betrieb einer kommunalen Musikschule)
- Weitergabe von Meldedaten an Dritte (z. B. an Mandatsträger zur Gratulation zu Alters- oder Ehejubiläen).

## Festlegung des Hauptwohnsitzes von Soldaten

Im Berichtszeitraum erhielt ich die Beschwerde eines Soldaten, der von der Meldebehörde aufgefordert worden war, einen Fragebogen zur Bestimmung der Hauptwohnung auszufüllen. Abgefragt wurden Daten über Familienstand, Arbeits- und Aufenthaltszeiten – sowohl am Heimatort als auch in der Kaserne – sowie weitere Daten (z. B. über Fahrtstreckenentfernungen, Fahrtzeiten und genutzte Verkehrsmittel zwischen diesen Unterkünften).

Meldebehörde entscheidet, was die Hauptwohnung ist

Wird die Kaserne für einen längeren Zeitraum als ein Jahr bezogen, ist sie als eine Wohnung anzusehen. Nutzt eine Person verschiedene Wohnungen, so obliegt es allein der Meldebehörde darüber zu entscheiden, welche Wohnung als Hauptwohnung anzusehen ist. Hierbei kommt es auf die tatsächlichen Aufenthaltszeiten (vorwiegende Nutzung) an. Lässt sich eine vorwiegende

1 § 37 Abs. 1 Bundesmeldegesetz

Nutzung nicht zweifelsfrei bestimmen, ist der Schwerpunkt der Lebensbeziehungen der meldepflichtigen Person entscheidend.

Zur Bestimmung der Hauptwohnung, darf die Meldebehörde die hierfür erforderlichen Daten erheben. Welche Daten erforderlich sind liegt allein im Ermessen der Behörde. Die Beschwerde war also unbegründet.

## Familienzusammenführung mit Hindernissen

Auskunftsersuchen zunächst ohne Erfolg

Ein Ordnungsamt hat Angehörige zur Übernahme der Beerdigungskosten einer Verstorbenen ermittelt: einen Sohn und einen Bruder der Verstorbenen. Mit der Aufforderung zur Kostenübernahme erfuhr der Bruder zum ersten Mal, dass er einen Neffen hatte. Der Name des Neffen wurde ihm allerdings nicht genannt.

Um Kontakt aufnehmen zu können, bat der Onkel das Ordnungsamt um die Kontaktdaten seines Neffen. Es gab dafür jedoch keine Rechtsgrundlage, da die Daten des Neffen nur zum Zweck der Kostenerstattung erhoben worden waren. Ebenso gelang es dem Onkel nicht, bei der Meldebehörde am letzten Wohnsitz der Verstorbenen eine Registerauskunft über seinen Neffen zu beantragen, da er ihn nicht namentlich benennen konnte. Da der Neffe bereits volljährig war, war auch kein Hinweis auf ihn im Datensatz der Verstorbenen gespeichert. Denn es werden nur die Daten von minderjährigen Kindern im Datensatz der Eltern gespeichert.

Um eine Familienzusammenführung dennoch zu ermöglichen, holte das Ordnungsamt vom Onkel eine Einwilligung ein, seine Daten an den Neffen zu übermitteln. So erhielt der Neffe die Möglichkeit eröffnet, sich selbst an seinen Onkel zu wenden.

## Anonymität auf Wunsch – Sperrvermerke für Bewohner von Pfiegeheimen

Betroffener muss vor Auskunft angehört werden

Für Personen, die in Pflegeheimen oder ähnlichen Einrichtungen wohnen, richtet die Meldebehörde einen bedingten Sperrvermerk gemäß § 52 BMG ein. Voraussetzung ist, dass die Behörde Kenntnis davon hat, dass es sich bei einer Anschrift um eine der im Gesetz aufgeführten Einrichtungen handelt. Eine Melderegisterauskunft über dort wohnende Personen darf nur erteilt werden, wenn die betroffene Person zuvor angehört wurde und schutzwürdige Interessen nicht beeinträchtigt werden. Die Meldebehörde muss sich jedoch nicht aktiv über in ihrem Zuständigkeitsgebiet ansässige Einrichtungen informieren.

Im Berichtszeitraum erreichte mich die Beschwerde eines vom Gericht bestellten Betreuers pflegebedürftiger Personen, die in einer Pflegeeinrichtung gemeldet sind. Die Meldebehörde hatte zu betreuten Bewohnern eine einfache Melderegisterauskunft erteilt, ohne dass die betroffenen Personen zuvor angehört worden waren. In sämtlichen Fällen waren allerdings keine Sperrvermerke vorhanden, da der Meldebehörde die Einrichtung nicht bekannt war.

## 4.4 Zählerstände ablesen – nicht alles, was interessant ist, ist erforderlich

Öffentliche Versorgungsverbände und private Unternehmen zur Energieversorgung ermitteln Verbrauchswerte mit Hilfe von Wasser- Gas- oder Stromzählern. Die Kunden können den Zählerstand selbst ablesen und ihn entweder auf einer Ablesekarte per Post oder in der Regel auch online per Formular an das Versorgungsunternehmen übermitteln. Hierbei dürfen jedoch nur Daten erhoben werden, die für die Abrechnung erforderlich sind. Bei Online-Angeboten sind entsprechende technische und organisatorische Maßnahmen Voraussetzung für eine datenschutzgerechte Verarbeitung der übermittelten Daten.

In einem Fall hatte ein Trinkwasserverband mit Hilfe der Ablesekarte neben dem Zählerstand auch die Telefonnummer, E-Mail-Adresse sowie die Unterschrift des Kunden erhoben. Ein Kunde bezweifelte die Erforderlichkeit der

abgefragten Daten. Zudem hatte er Bedenken, die Ablesekarte im offenen Postversand zurückzusenden. Er befürchtete, dass unbefugte Dritte Kenntnis über seine Daten erlangen könnten.

Bedenken gegen Postkarten

## Schutz durch das Postgeheimnis

Diese Sorge ist jedoch unnötig, da die angegebenen personenbezogenen Daten nach Absendung der Ablesekarte dem Post- und Fernmeldegeheimnis unterliegen. Damit ist sichergestellt, dass die Karten auf dem Transportweg nicht von Unbefugten gelesen werden. Der generelle Einsatz von Postkarten zur Zählerstandübermittlung ist also datenschutzrechtlich in Ordnung.

Mit Blick auf die über den Zählerstand hinaus erfragten Daten sah es allerdings anders aus. Ich habe den Trinkwasserverband darauf hingewiesen, dass es sich bei Telefonnummer und E-Mail-Adresse um Daten handelt, die nicht für die Verbrauchsabrechnung erforderlich sind, da der Kunde auch über die Wohnanschrift kontaktiert werden kann. Der Trinkwasserverband hat daraufhin die Gestaltung seiner Ablesekarten geändert. Telefonnummer und E-Mail-Adresse können nun freiwillig angegeben werden.

Telefon und E-Mail nicht erforderlich

## Zählerstände per Online-Formular nur verschlüsselt zulässig

Bei der Einrichtung von Online-Formularen sind grundsätzlich technische und organisatorische Maßnahmen zu treffen, die eine datenschutzgerechte Verarbeitung der Daten sicherstellen. In einem Fall hatte ein Trinkwasserverband ein Formular angeboten, mit dem die Kundendaten unverschlüsselt übermittelt wurden. Nachdem ich auf die erforderliche Verschlüsselung hingewiesen hatte, nahm der Verband das Angebot umgehend von seiner Homepage. Er sagte zu, für die Ablesung im Folgejahr ein verschlüsseltes Angebot zur Verfügung zu stellen.

Verband sagt Nachbesserung zu

# 4.5 Selbstbedienungsterminals im Bürgerbüro – kundenfreundlich, aber auch datenschutzgerecht?

Um Bürgern die Beantragung von Personalausweisen zu erleichtern und Bearbeitungszeiten zu verkürzen, bieten viele Kommunen inzwischen Selbstbedienungsterminals direkt im Bürgerbüro oder vor dem Rathaus an. Soweit ein Terminal Eigentum der Kommune ist, werde keine Daten an Dritte übermittelt. Werden auch entsprechende technisch-organisatorische Maßnahmen eingehalten, ist der Einsatz unbedenklich. Wird das Gerät aber geleast oder gemietet, muss die Kommune mit dem Dienstleister einen Vertrag über die Auftragsverarbeitung schließen.

Selbstbedienungsterminals dienen der Erfassung, Prüfung und Übermittlung von Daten für hoheitliche Dokumente (z. B. Personalausweise). So hat ein Bürger etwa am Terminal die Möglichkeit, alle für den Personalausweis notwendigen personenbezogenen Daten wie Lichtbild und Fingerabdrücke zu erfassen. Die Daten werden anschließend zusammen mit dem Geburtsdatum gespeichert und in das Fachverfahren des Bürgeramtes übermittelt. Dort können die Daten vom jeweiligen Sachbearbeiter abgerufen werden. Nach dem Abruf, werden die Daten aus dem Arbeitsspeicher des Selbstbedienungsterminals gelöscht. Auch niedersächsische Kommunen interessierten sich für ein solches Terminal und baten mich um Beratung.

Nach Abruf werden die Daten aus den Terminals gelöscht

## Voraussetzungen für die Datenverarbeitung

Sowohl die Erhebung der personenbezogenen Daten als auch ihre Übermittlung vom Terminal in das Fachverfahren des Bürgeramtes müssen rechtlich zulässig sein. Die Personalausweisverordnung (PAuswV) regelt die Erhebung und weitere Verarbeitung des Lichtbildes. Wenn die Personalausweisbehörde die technischen Voraussetzungen geschaffen hat, kann das Lichtbild auch von Dritten elektronisch an die Behörde übermittelt werden oder durch die Behörde selbst gefertigt werden[1].

Erfassung der Fingerabdrücke auf Antrag

Die Fingerabdrücke werden elektronisch erfasst. Dies ist nur mit Einwilligung der betroffenen Person und auf deren Antrag möglich[2]. Die Erfassung der personenbezogenen Daten erfolgt anonymisiert und die Datenübermittlung an das Fachverfahren im Bürgeramt ist verschlüsselt, sodass für die Datenverarbeitung keine datenschutzrechtlichen Bedenken bestehen.

Was die Einhaltung technisch-organisatorischer Maßnahmen beim Einsatz von Terminals angeht, so dürfen die Daten nur mit Geräten übermittelt werden, die durch das Bundesamt für Sicherheit und Informationstechnik zertifiziert sind.

## Mieten, Leasen oder Kaufen?

Vertrag mit dem Dienstleister nötig

Wird das Terminal gemietet oder geleast, werden personenbezogene Daten auf dem Gerät des Dienstleisters verarbeitet. Die Daten müssen dann vom Dienstleister an die Kommune übermittelt werden. In diesen Fällen liegt eine Auftragsverarbeitung vor, für die ein Vertrag zwischen der Kommune und dem Dienstleister notwendig ist. Bei der Rückgabe gemieteter oder geleaster Geräte ist darauf zu achten, dass sich keine personenbezogenen Daten mehr im Speicher des Geräts befinden dürfen und die Daten vor Rückgabe vollständig gelöscht werden.

Kauf am sichersten

Ist die Kommune selbst Eigentümer des Selbstbedienungsterminals, werden die gesamten Daten durch die Kommune verarbeitet. Da keine Dritten beteiligt sind, ist der Kauf die datenschutzgerechteste Variante.

1 § 7 Abs. 1 Satz 2 PAuswV

2 § 5 Abs. 9 Personalausweisgesetz

## 4.6 Veröffentlichung von Archivdaten zu Forschungszwecken

Von einer Gemeinde wurde mir die Frage gestellt, wie die Veröffentlichung personenbezogener Daten aus Archiven von Personen, die Opfer von NS-Medizinverbrechen wurden, rechtlich zu bewerten sei. Geplant war die Lebensdaten (Geburts- und Sterbedatum, Geburts- und Sterbeort) der Opfer in einem Erinnerungsbuch und auf einem Gedenkstein zu veröffentlichten. Dies ist nur mit Einwilligung der Angehörigen der Opfer zulässig.

Die Nutzung von Archivmaterial wird durch das Niedersächsische Archivgesetz (NArchG) geregelt und erfolgt auf Antrag zu wissenschaftlichen Zwecken oder bei sonst berechtigtem Interesse. Handelt es sich wie im vorliegenden Fall um Informationen zu einer betroffenen Person, deren Geburts- oder Sterbedatum bekannt oder mit vertretbarem Aufwand aus diesem Archiv zu ermitteln ist, so darf das Archivmaterial frühestens zehn Jahre nach dem Tode dieser Person genutzt werden. Falls das Sterbedatum nicht feststellbar ist, darf das Material 100 Jahre nach deren Geburt verwendet werden.

Interessen der Angehörigen beachten

Zudem sind schutzwürdige Interessen betroffener Personen, soweit sie ohne besonderen Aufwand erkennbar sind, angemessen zu berücksichtigen. Betroffene Personen sind im vorliegenden Fall vor allem lebende Angehörige der Menschen, deren Lebensdaten veröffentlicht werden sollen.

Da es sich bei den Personen, deren Daten veröffentlicht werden sollen, um Opfer von NS-Medizinverbrechen handelt, ist davon auszugehen, dass schutzwürdige Belange der Angehörigen betroffen sind. Eine Veröffentlichung der Lebensdaten ist daher nur mit deren vorheriger Einwilligung datenschutzrechtlich zulässig.

# 4.7 Melderegisterauskunft – Behörden kommen ihrer Pfiicht nicht nach

Meldebehörden dürfen eine einfache Melderegisterauskunft zu einer Person nur erteilen, wenn die Auskunft verlangende Person oder Stelle versichert, dass sie die Daten nicht für Werbung oder zum Adresshandel verwenden wird. Ausnahme: Die Person, deren Daten erfragt werden, hat in eine entsprechende Verwendung eingewilligt. Das müssen die Behörden überprüfen, tun sie häufig aber nicht.

Behörde muss Einwilligungen prüfen

Nach Bundesmeldegesetz (BMG) darf eine anfragende Person oder Stelle nur eine Melderegisterauskunft erhalten, wenn

- sie eine Erklärung abgibt, dass sie die erfragten Daten nicht für Zwecke der Werbung oder des Adresshandels verwenden wird oder
- versichert, ihr liege von der Person, deren Daten erfragt werden, eine Einwilligung vor, dass ihre Daten zu Zwecken der Werbung oder des Adresshandels verwendet werden dürfen.

Gemäß § 44 Abs. 3 Satz 6 BMG müssen die Meldebehörden stichprobenartig überprüfen, ob Einwilligungserklärungen der beantragenden Person tatsächlich vorliegen. Mit einer Prüfung unter 50 Meldebehörden habe ich mich der Frage gewidmet, wie viele von ihnen dies tatsächlich kontrollieren.

Defizite bei 35 von 50 Meldebehörden

Das Ergebnis: Nur 15 der 50 geprüften Meldebehörden handeln datenschutzkonform. Die übrigen Behörden haben entweder nicht erkannt, in welchen Fällen eine Überprüfung durchzuführen ist oder sie sind ihrer Pflicht zur stichprobenhaften Kontrolle nicht nachgekommen. Ich habe die betroffenen Meldebehörden schriftlich über das geltende Recht aufgeklärt und sie auf ihre gesetzlichen Pflichten hingewiesen.

# 4.8 Standesämter – Prüfung zur Datenweitergabe für wissenschaftliche Zwecke

Standesämter dürfen unter bestimmten Voraussetzungen Hochschulen, anderen Forschungseinrichtungen und öffentlichen Stellen Auskunft aus dem Personenstandsregister gewähren. Ob diese Voraussetzungen vorliegen, müssen die Ämter eigenständig überprüfen. Ob sie dieser Pflicht vor der Erteilung einer Auskunft nachkommen, habe ich bei 40 Standesämtern kontrolliert. Die Prüfung offenbarte, dass teilweise erhebliche Unsicherheiten bestehen.

Gemäß § 66 Abs. 1 Personenstandsgesetz (PStG) ist die Auskunftserteilung an die folgenden Voraussetzungen gebunden:

Voraussetzungen für die Auskunftserteilung

- Sie muss für die Durchführung bestimmter wissenschaftlicher Forschungsvorhaben erforderlich sein,
- eine Nutzung anonymisierter Daten zu diesem Zweck darf nicht möglich oder die Anonymisierung muss mit einem unverhältnismäßigen Aufwand verbunden sein,
- das öffentliche Interesse an der Durchführung des Forschungsvorhabens muss die schutzwürdigen Belange des Betroffenen an dem Ausschluss der Benutzung erheblich überwiegen,
- die empfangende Stelle muss die technischen und organisatorischen Maßnahmen treffen, die nach datenschutzrechtlichen Vorschriften zum Schutz von Daten erforderlich und angemessen sind und
- es muss eine Zustimmung der für den Fachbereich des Forschungsvorhabens zuständigen obersten Bundes- oder Landesbehörde oder einer von dieser bestimmten Stelle vorliegen.

Die Erteilung einer Auskunft erfolgt nur, wenn das Standesamt das Vorliegen sämtlicher Voraussetzungen geprüft hat.

## Nur selten Forschungsanfragen an Standesämter

Meine Prüfung hat ergeben, dass nur 3 von 40 Standesämtern Auskunftsersuchen zu Forschungszwecken vorlagen. Die Antworten dieser Ämter ließen jedoch erkennen, dass sie den Regelungsinhalt des § 66 PStG nicht erkannt haben.

Eigenständige Prüfung und Zustimmung nötig

So regelt § 66 Abs. 1 Satz 1 PStG eine eigenständige Prüfung durch die Standesämter. Zusätzlich fordert § 66 Abs. 2 PStG eine Zustimmung durch die für das Forschungsvorhaben zuständige oberste Bundes- oder Landesbehörde. Die Standesämter nahmen jedoch unzutreffend an, dass bei Vorliegen dieser Zustimmung keine eigenständige Prüfung mehr notwendig sei.

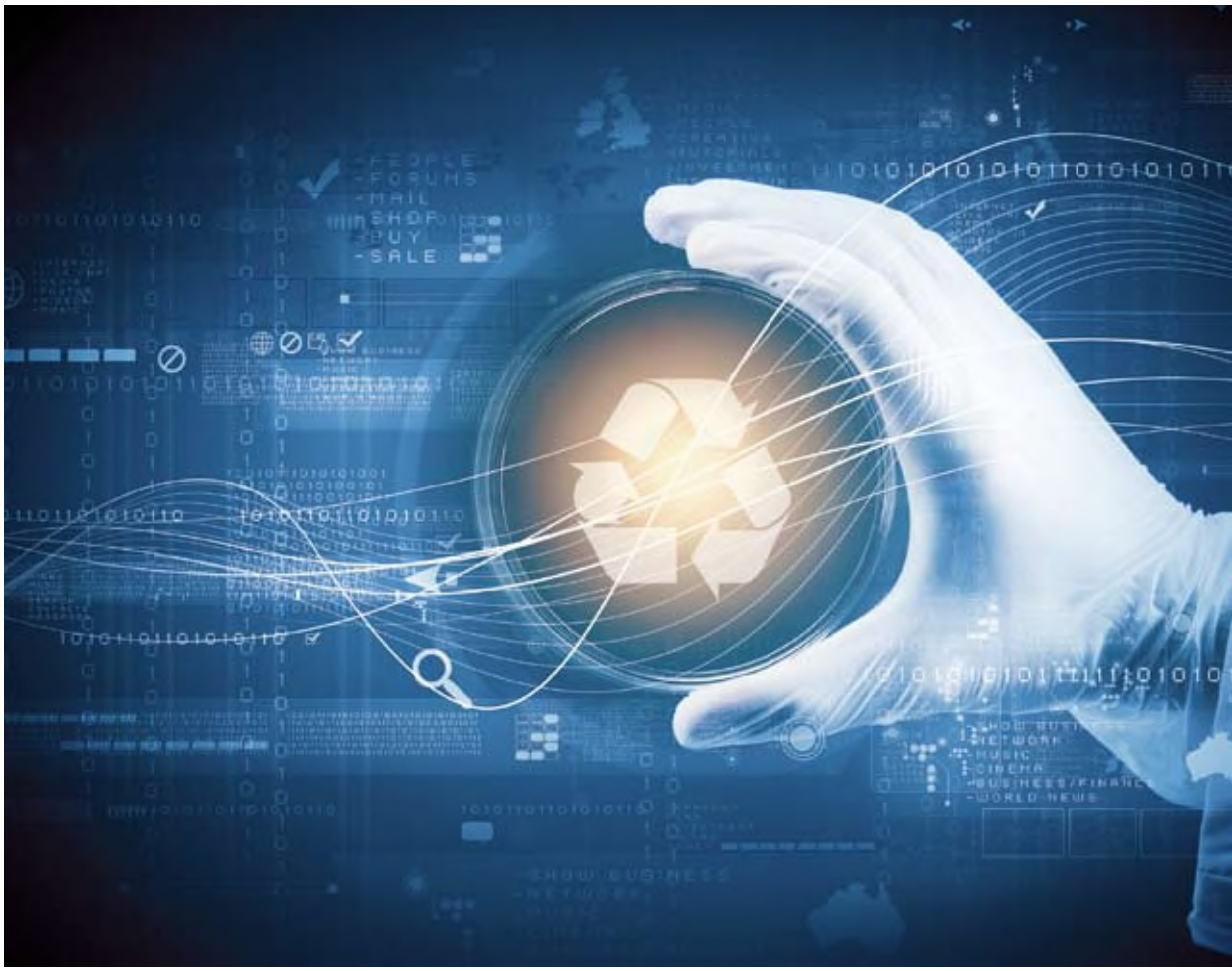
Ich habe die betroffenen Standesämter schriftlich über das geltende Recht aufgeklärt und auf die bestehenden gesetzlichen Pflichten hingewiesen.

# 4.9 Prüfung zum Datenschutz auf dem Abfallhof

Bei der Anlieferung von Müll auf Abfallhöfen werden personenbezogene Daten der Kunden mithilfe des Personalausweises oder des Kfz-Kennzeichens kontrolliert. Durch diese Datenverarbeitung soll sichergestellt werden, dass nur Personen ihren Müll anliefern, die auch tatsächlich im Einzugsgebiet des Abfallhofes wohnen. Wichtig ist jedoch, dass die Entsorgungsträger nur die Daten verarbeiten, die für Abwicklung der Abfallentsorgung erforderlich sind. Ob diese Vorgabe eingehalten wird, habe ich mit einer schriftlichen Überprüfung bei 24 Entsorgungsträgern kontrolliert.

Kennzeichen in allen Fällen erforderlich

Sämtliche befragten Entsorgungsträger gaben an, die Kfz-Kennzeichen der anliefernden Kunden zu kontrollieren. Diese Datenverarbeitung war auch in allen Fällen erforderlich.



Die Hälfte der Befragten gab an, neben dem Kennzeichen auch Angaben aus dem Personalausweis oder einem anderen Identifikationspapier der Kunden zu verarbeiten. Die Verarbeitung der Angaben aus Identifikationspapieren ist allerdings nur für folgende Zwecke erforderlich:

- Rechnungserstellung für die Abfallanlieferung
- Nachweisführung gemäß abfallrechtlicher Vorschriften bei Anlieferung bestimmter Abfallarten
- Feststellung der Abfallherkunft gemäß abfallrechtlicher Vorschriften
- Feststellung der Gebietszugehörigkeit, wenn diese nicht bereits auf Grund des Kfz-Kennzeichens festgestellt werden kann

## Ausweisdaten für Gebühren nicht nötig

Grundsatz der Erforderlichkeit

Für die Gebührenbemessung ist die Verarbeitung von Angaben aus dem Personalausweis nicht erforderlich. Dieser Zweck kann durch die Nutzung der weniger sensiblen Informationen des Kfz-Kennzeichens erreicht werden. Insofern verstößt die Verarbeitung von Angaben aus dem Personalausweis zu Zwecken der Gebührenbemessung gegen den Grundsatz der Erforderlichkeit des Niedersächsischen Abfallgesetzes (§ 45 Abs. 1).

## Löschpfiichten nicht hinreichend beachtet

Grundsatz der Speicherbegrenzung

Eine Vielzahl der Entsorgungsträger gab an, trotz Ablauf gesetzlicher Aufbewahrungsfristen, die gespeicherten Daten aus Kfz-Kennzeichen sowie Daten aus Personalausweisen nicht zu löschen. Dies stellt jedoch einen datenschutzrechtlichen Verstoß gegen den Grundsatz der Speicherbegrenzung dar.

## Informationspfiichten werden nicht umgesetzt

Nur 2 von 24 Entsorgungsträgern erfüllten die ihnen obliegenden Verpflichtungen, ihre Kunden über die Verarbeitung ihrer personenbezogenen Daten hinreichend zu informieren. Auch das stellt einen datenschutzrechtlichen Verstoß dar.

Prüfung zeigt deutliche Mängel

Insgesamt ist das Prüfungsergebnis als datenschutzrechtlich ungenügend zu bewerten. Die Mehrzahl der geprüften Abfallentsorger erhebt mehr Daten als notwendig, verstößt im Anschluss gegen Löschfristen oder informiert die Kunden nur unzureichend über die Verarbeitung der erhobenen Daten.

Ich habe die betroffenen Entsorgungsträger über das geltende Recht aufgeklärt und sie auf ihre gesetzlichen Pflichten hingewiesen.

# F.5. Datenschutz in der Schule

## 5.1 Verwendung von WhatsApp in der Schule

„WhatsApp" zählt zu den beliebtesten Messenger-Diensten für die private Kommunikation. Da liegt es nahe, dieses fast überall vorhandene Programm auch im schulischen Bereich verwenden zu wollen. Ich betrachte es allerdings als unzulässig, wenn Lehrkräfte sowohl untereinander als auch mit den Schülern und deren Erziehungsberechtigten per WhatsApp kommunizieren.

Bereits bei der Anmeldung zu diesem Messenger-Dienst werden alle im Telefon des Nutzers gespeicherten Kontaktdaten an den Anbieter übertragen. Hierzu besteht weder eine Rechtsgrundlage noch können die Personen, die im Nutzertelefon gespeichert sind, in die Datenweitergabe einwilligen oder ihr widersprechen.

Im Oktober 2017 habe ich die Unzulässigkeit von WhatsApp in Schulen in einem Merkblatt auf meiner Website thematisiert. Gleichzeitig übersandte ich das Merkblatt an das Kultusministerium zur Information der Schulen.

Merkblatt – Kurzlink: https://t1p.de/WhatsApp-Schule

### Keine Datenverarbeitung auf privaten Geräten

Zwar ermöglichen Dienste wie WhatsApp einen unkomplizierten und direkten Informationsaustausch im Schulalltag. Das kann aufgrund der datenschutzrechtlichen Probleme aber nicht als Argument für deren Einsatz dienen. Zudem dürfen Lehrkräfte private Geräte nicht für die Verarbeitung dienstlicher personenbezogener Daten nutzen, insbesondere von Kontaktdaten. Daher stellen auch andere Messenger keine geeignete Alternative zu WhatsApp dar.

Meine Empfehlung an die Schulen lautet daher, dass Informationen zwischen Lehrkräften untereinander sowie mit ihren Schülern und deren Eltern ausschließlich über eine schulische E-Mail-Adresse ausgetauscht werden sollten. Selbstverständlich müssen auch hier die Vorgaben des Datenschutzes eingehalten werden.

Empfehlung: Schulische E-Mail-Adresse

## Kontrolle zu Kommunikation an Schulen

Auch nach der Veröffentlichung des Merkblatts erreichten mich noch viele Anfragen aus den Schulen zu diesem Thema. Deshalb habe ich die Schulen noch einmal direkt über die Unzulässigkeit von WhatsApp informiert. Im 4. Quartal 2018 habe ich zudem 70 zufällig ausgewählte Schulen gebeten, mir einen Fragenkatalog zur Kommunikation an den jeweiligen Einrichtungen zu beantworten.

Einige verwenden weiterhin WhatsApp

Diese Kontrolle konnte ich im Berichtszeitraum zwar nicht abschließen. Die bereits eingegangenen Rückläufe zeigen jedoch, dass das Datenschutzbewusstsein noch nicht überall angekommen ist: An einigen Schulen nutzen Lehrinnen und Lehrer WhatsApp weiter für die dienstliche Kommunikation. An diesen Schulen werde ich daher separate Kontrollverfahren einleiten.

# 5.2 Niedersächsische Bildungscloud ohne Datenschutzkonzept

Zur Digitalisierung des Unterrichts will die Niedersächsische Landesregierung eine eigene Bildungscloud einrichten. Datenschutz und Datensicherheit sollten bei diesem Projekt besondere Aufmerksamkeit genießen. Daher habe ich gefordert mein Haus frühzeitig in die Entwicklung einzubinden. Doch ein prüfbares Datenschutzkonzept konnte mir bis jetzt nicht vorgelegt werden.

Die Entwicklung einer Niedersächsischen Bildungscloud als kollaborative digitale Lern- und Arbeitsumgebung ist Teil der Digitalisierungsstrategie der Landesregierung. Das Niedersächsische Kultusministerium hat bereits im Jahr 2016 die Landesinitiative „n-21: Schulen in Niedersachsen online e.V." mit der Entwicklung beauftragt. In mehreren Besprechungen haben meine Mitarbeiter darauf hingewiesen, dass zwingend ein Datenschutzkonzept vorgelegt werden muss, wenn die Bildungscloud durch mich geprüft und anschließend datenschutzkonform betrieben werden soll.

## Weiterentwicklung von bundesweiter Schulcloud

Kooperation mit Hochschulinstitut

Im Rahmen der Bildungsmesse „didacta" verkündete der Niedersächsische Kultusminister im Februar 2018 eine Kooperation mit einem Hochschulinstitut. Dieses entwickelt derzeit eine eigene Schulcloud, die bundesweit zum Einsatz kommen soll. Auf Nachfrage wurde erklärt, dass die Niedersächsische Bildungscloud eine Weiterentwicklung dieser Schulcloud sein soll. Nähere Spezifizierungen stehen aber aus.
Zudem konnte auch die bundesweite Schulcloud bislang noch nicht durch die Datenschutzaufsichtsbehörden bewertet werden. Denn erst zum Ende des Berichtszeitraumes wurde ein Datenschutzkonzept vorgelegt. Ein Unterarbeitskreis der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder wird es bewerten.

## Auch Pilotbetrieb muss Datenschutz beachten

Angesichts der erheblichen zeitlichen Verzögerungen habe ich das Kultusministerium und n-21 mehrfach auf Folgendes hingewiesen: Auch der Pilotbetrieb einer Schulcloud darf nur unter Beachtung der datenschutzrechtlichen Anforderungen erfolgen, sofern hier mit Echtdaten der Schülerinnen und Schüler gearbeitet wird.
Dies gilt insbesondere seit Geltung der Datenschutz-Grundverordnung. Denn diese macht neben den allgemeinen rechtlichen Anforderungen auch konkrete Vorgaben zu technisch-organisatorischen Maßnahmen einschließlich der Erstellung einer Datenschutzfolgenabschätzung.

Konkrete Vorgaben zu technisch-organisatorischen Maßnahmen

# 5.3 Hilfe zum Einsatz eines elektronischen Klassenbuchs

Statt des herkömmlichen Klassenbuchs in Papierform gibt es inzwischen auch eine Vielzahl digitaler Alternativen. Grundsätzlich erlaubt das Niedersächsische Schulgesetz die Nutzung eines elektronischen Klassenbuchs, wenn die Anforderungen des Datenschutzes eingehalten werden. Wegen der gestiegenen Nachfrage habe ich auf meiner Website einen entsprechenden Leitfaden für die Schulen veröffentlicht.

Hinweise zur Einführung – Kurzlink: https://t1p.de/Klassenbuch

Kerninhalte des Leitfadens sind

- zum einen die erforderliche datenschutzrechtliche Prüfung vor der Einführung des Klassenbuchs und
- zum anderen der Hinweis, dass die grundsätzlich zulässig gespeicherten Daten nicht auf privaten mobilen Endgeräten (Smartphone, Tablet) gespeichert werden dürfen.

Weiterhin ist darauf zu achten, dass nur die Daten erhoben werden, die auch für das Klassenbuch in Papierform erforderlich sind. Da dort beispielsweise keine Noten eingetragen werden dürfen, ist dies auch im elektronischen Klassenbuch nicht zulässig.

Keine Noten eintragen

## Großes Interesse – geringe Anwendung

Prüfung an 70 Schulen

Die weiter hohe Zahl der Anfragen aus den Schulen zu diesem Thema hat mich veranlasst, die Schulen noch einmal direkt über die Voraussetzungen für ein elektronisches Klassenbuch zu informieren. Im 4. Quartal 2018 habe ich zudem 70 zufällig ausgewählte Schulen gebeten, mir einen Fragenkatalog zur Kommunikation an den jeweiligen Institutionen zu beantworten.

Die Auswertung konnte ich im Berichtszeitraum nicht abschließen. Die bereits eingegangenen Rückläufe zeigen jedoch, dass zumindest bei den angefragten Schulen das elektronische Klassenbuch noch nicht sehr weit verbreitet ist. Trotz des großen Interesses hat die elektronische Variante der Papierform bislang also noch nicht den Rang abgelaufen.

In Einzelfällen hat sich bei meiner Prüfung allerdings gezeigt, dass in der digitalen Variante mehr Daten als im herkömmlichen Klassenbuch gespeichert werden, beispielsweise Fotos der Schülerinnen und Schüler. Eine Speicherung von Bilddateien ist aber weder notwendig noch zulässig. Aus diesem Grund werde ich an diesen Schulen separate Kontrollverfahren einleiten.

Weitere Kontrollverfahren nötig

# 5.4 Datenschutzkonformer Einsatz von Tablets im Schulunterricht

Der Einsatz von Tablets im Schulunterricht setzt geeignete Konzepte voraus, damit die Schulen als verantwortliche Stellen die Risiken für Datenschutz und -sicherheit beherrschen können. Ich habe im Oktober 2018 Eckpunkte für einen datenschutzkonformen Einsatz von Tablets im Schulunterricht veröffentlicht.

Das Lernen mit und über neue Medien ist aus pädagogischer Sicht uneingeschränkt zu begrüßen. An vielen niedersächsischen Schulen sind sogenannte Tablet-Klassen eingerichtet. In diesen werden entweder landeseigene Tablets bereitgestellt oder aber die Schüler nutzen ihre eigenen Geräte nach dem Bring-Your-Own-Device-Konzept (BYOD). Letzteres wird vom Niedersächsischen Kultusministerium favorisiert.

Land favorisiert BYOD

## Sicherer Server der Schule nötig

Bereits im Tätigkeitsbericht 2015/2016 habe ich ausgeführt, dass landeseinheitliche Rahmenbedingungen für den Einsatz von Tablets im Schulunterricht erforderlich sind. Gerade bei BYOD besteht die Gefahr, dass private und schulische Inhalte vermischt werden. Damit entstehen besondere Risiken für die personenbezogenen Daten der Schüler. Aus diesem Grund ist die Nutzung privater mobiler Endgeräte u.a. nur dann akzeptabel, wenn keinerlei Daten auf dem Gerät selbst gespeichert werden, sondern ausschließlich auf einem gesicherten Server der Schule.

Risiken für Daten der Schüler

Das Niedersächsische Landesinstitut für schulische Qualitätsentwicklung (NLQ) hat im Jahr 2016 den Entwurf eines Leitfadens zum Einsatz mobiler Computer im Schulunterricht vorgelegt. Dieser beruhte jedoch auf dem „alten" Niedersächsischen Datenschutzgesetz vor Geltung der Datenschutz-Grundverordnung, sodass sich in der Zwischenzeit noch erheblicher Nachbesserungsbedarf ergab.

Um den Schulen kurzfristig die erforderlichen Informationen bereitzustellen, habe ich deshalb im September 2018 eigene Eckpunkte zum datenschutzkonformen Einsatz von Tablets im Schulunterricht formuliert und auf meiner Website veröffentlicht. Ich habe dem NLQ empfohlen, diese Eckpunkte bei der Finalisierung seines Leitfadens zu berücksichtigen.

Eckpunkte – Kurzlink: https://t1p.de/Tablets-im-Unterricht

# 5.5 DigLu – Digitales Lernen unterwegs

Mit der länderübergreifenden Online-Plattform „Digitales Lernen unterwegs“ (DigLu) können beruflich reisende Eltern die Schulbesuche ihrer Kindern organisieren. Die Plattform ermöglicht die Kontaktaufnahme zu Lehrkräften und gibt einen Überblick zum aktuellen Lernstand der Kinder. Da Niedersachsen an der Pilotphase teilnehmen wird, habe ich gemeinsam mit weiteren Aufsichtsbehörden meine Beratung angeboten.

Das Projekt DigLu ist Bestandteil der Strategie der Kultusministerkonferenz (KMK) „Bildung in der digitalen Welt“. In einer Pilotphase soll ab dem Schuljahr 2019/2020 zunächst in sechs Ländern ein gemeinsames Konzept zur Unterrichtsgestaltung für Kinder beruflich Reisender umgesetzt werden. Mittelfristig sollen weitere Länder beitreten.

Erweiterung des analogen Schultagebuchs

Kern des Konzepts ist eine Lernplattform und eine Schulorganisationssoftware, auf die online zugegriffen werden kann. Dabei werden die Funktionalitäten des herkömmlichen analogen Schultagebuchs um die Möglichkeiten digitalen Lernens und digitaler Kommunikation erweitert.

## Plattform noch ohne Datenschutzkonzept

Unterlagen müssen überarbeitet werden

In Niedersachsen soll DigLu von zehn Prozent der Kinder beruflich reisender Eltern in einer Pilotphase getestet werden. Daher habe ich zusammen mit weiteren Aufsichtsbehörden der zuständigen Arbeitsgruppe der KMK eine datenschutzrechtliche Beratung angeboten. Dabei stellte sich heraus, dass ein prüfbares Datenschutzkonzept noch nicht vorliegt. Auch die bereits vorgelegten Unterlagen müssen noch einmal überarbeitet werden. Dies betrifft vor allem die Mustererklärungen zur Einwilligung sowie die Frage, in welcher rechtlichen Beziehung die Pilotländer und Schulen zu weiteren Akteuren und Auftragsnehmern stehen.

Federführung liegt bei NRW

Die Federführung der teilnehmenden Kultusministerien liegt bei Nordrhein-Westfalen. Erst wenn dort ein prüfbares Datenschutzkonzept vorgelegt wurde, werden die Aufsichtsbehörden das Projekt begleiten können. Jedoch immer nach dem Grundsatz, dass Echtdaten von Schülern auch im Pilotbetrieb nur verarbeitet werden dürfen, wenn die Anforderungen des Datenschutzes erfüllt werden.

# F.6. Gesundheit und Soziales

## 6.1 Klinisches Krebsregister: Widerspruchsmöglichkeit bleibt unzureichend

Ende gut, alles gut beim Klinischen Krebsregister Niedersachsen? Leider nicht ganz. Im Rahmen der mehrjährigen Begleitung des Gesetzgebungsverfahrens wurden zwar zahlreiche datenschutzrechtliche Forderungen meiner Behörde umgesetzt, ein aus meiner Sicht wesentlicher Punkt blieb jedoch offen – das umfassende Widerspruchsrecht der Betroffenen.

Auch in den vergangenen zwei Jahren habe ich das Gesetzgebungsverfahren zum Gesetz über das Klinische Krebsregister Niedersachsen (GKKN) sowie die in diesem Zusammenhang erlassenen Verordnungen genauso weiter begleitet, wie den Aufbau des technisch-organisatorischen Datenschutzes in der neu gegründeten Anstalt des KKN.

Sorgfältige Interessenabwägung nötig

Bereits beim Gesetz über das Epidemiologische Krebsregister Niedersachsen (GEKN)[1] musste sorgfältig abgewogen werden: Zwischen dem Interesse der Allgemeinheit an einer möglichst vollzähligen Erfassung von Krebserkrankungen auf der einen Seite, um mögliche Ursachen sowie schädliche regionale Umwelteinflüsse identifizieren zu können und dem Recht auf informationelle Selbstbestimmung der Betroffenen auf der anderen. Um die Aussagekraft des Registers zu erhöhen, wurde erstmalig eine uneingeschränkte Meldepflicht in das Gesetz aufgenommen.

### Pseudonyme im epidemiologischen Register

Die Daten im Epidemiologischen Krebsregister (EKN) werden ausschließlich pseudonymisiert (per Kontrollnummer) gespeichert. Zur Wahrung ihres Rechts auf informationelle Selbstbestimmung wurde den Betroffenen das Recht eingeräumt, der dauerhaften Speicherung ihrer Identitätsdaten, unabhängig ob im Klartext oder als Chiffrat, zu widersprechen.

1 22. Tätigkeitsbericht (ab Seite 48)

Behandlung dokumentieren und verbessern

Im Gegensatz zum EKN hat das KKN vereinfacht dargestellt zum einen den Zweck, Behandlungsverläufe von allen Krebserkrankungen in Niedersachsen zu dokumentieren, um die Krebsbehandlung insgesamt zu verbessern. Zum anderen soll es die Krebserkrankungsdaten für die individuelle Behandlung der einzelnen Betroffenen zur Verfügung stellen. Aus diesem Grund müssen die Daten im KKN personenbezogen erfasst werden.[2]

## Schwerwiegenderer Eingriff im klinischen Register

Während der Nutzen des KKN für die Allgemeinheit zumindest ähnlich hoch zu werten ist wie beim EKN, so stellt diese Art der Speicherung und Nutzung der personenbezogenen Gesundheitsdaten im KKN einen wesentlich schwerwiegenderen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Die vom Gesetzgeber im GKKN vorgesehene Widerspruchsmöglichkeit sieht jedoch kein Recht auf Löschung der personenbezogenen Daten vor, sondern lediglich eine Einschränkung der Datenverarbeitung.

Kein Recht auf Löschung vorgesehen

Aufgrund der Sensibilität der Daten wäre eine Widerspruchsregelung, ähnlich der des GEKN daher ausdrücklich zu begrüßen gewesen. In meiner Stellungnahme zum Gesetzentwurf habe ich der Landesregierung sowie den zu diesem Zeitpunkt im Niedersächsischen Landtag vertretenen Fraktionen verschiedene Argumente für eine datenschutzfreundliche und gegen die im Gesetzentwurf enthaltene Widerspruchsregelung vorgetragen. Leider wurden meine Empfehlungen in diesem Punkt nicht umgesetzt.

Landtag folgt nicht meinen Empfehlungen

Die übrigen Vorschriften des GKKN sowie die dazu gehörigen Verordnungen sind mit mir abgestimmt.

Das GKKN ist zum 1. Dezember 2017 in der aktuellen Fassung in Kraft getreten.

2 § 65c Abs. 1 Nr. 1 SGB V

## 6.2 Prüfung von Wohngeldstellen stellt maßlose Datenerhebung fest

Wohngeldstellen dürfen für das Wohngeldverfahren in der Regel nur die per Erlass[1] des Sozialministeriums vorgeschriebenen amtlichen Formblätter verwenden. Eine Prüfung offenbarte jedoch den unzulässigen Einsatz zusätzlicher Formblätter.

Ergänzende Angaben gefordert

Durch Eingaben bin ich darauf aufmerksam gemacht worden, dass einige Wohngeldstellen in Niedersachsen neben den vorgeschriebenen Wohngeldvordrucken ein weiteres Formblatt mit der Bezeichnung „Ergänzende Angaben über die Einnahmen und Ausgaben“ oder ein vergleichbares Formular verwenden.

1 RdErl. d. MS v. 10. 11. 2015 – 506-25 340-22/4 – VORIS 23400 —

Darin werden die Antragstellenden aufgefordert, zusätzlich zu ihrem Wohngeldantrag, in dem sie bereits Angaben zur Miete machen, nochmals ihre monatlichen Mietausgaben und darüber hinaus weitere Ausgaben anzugeben. Zum Beispiel zur Ernährung (Frühstück, Mittag- und Abendessen), zu persönlichen Dingen des täglichen Lebens (Kosmetik, Körperpflege, Zeitschriften, Bücher, Vereine, Hobby, Kino usw.) und zu Neuanschaffungen (Bekleidung usw.).

## Daten nicht für Aufgabenerfüllung nötig

Meine stichprobenartige Überprüfung von 19 Wohngeldstellen in ganz Niedersachsen hat ergeben, dass 11 der angeschriebenen Stellen ein unzulässiges Formblatt verwenden.

Doppelte und zu umfangreiche Erhebung

Aus datenschutzrechtlicher Sicht ist eine routinemäßige Verwendung eines solchen bzw. eines vergleichbaren Vordrucks, die nicht auf Freiwilligkeit beruht, unzulässig. Zum einen werden Daten doppelt erhoben, zum anderen werden Daten erfragt, die in diesem Umfang nicht für die Aufgabenerfüllung erforderlich sind – ohne Hinweis auf die Freiwilligkeit oder die Möglichkeit eines anderweitigen Nachweises der Bedürftigkeit.

Nur für den Fall, dass sich bei der Ermittlung des Jahreseinkommens Einnahmen unterhalb des Sozialhilfesatzes ergeben, kann den Antragstellenden als Hilfsmittel für den Nachweis des Wohngeldanspruchs eine zusätzliche Checkliste zur Verfügung gestellt werden. Das Ausfüllen dieser Liste darf jedoch nicht verpflichtend sein. Die Antragstellenden sind ausdrücklich darauf hinzuweisen, dass auch andere Möglichkeiten für den Nachweis der Plausibilität in Betracht kommen.

## Ministerium veröffentlicht Runderlass

Nachdem ich das Niedersächsische Ministerium für Soziales, Gesundheit und Gleichstellung über die unzulässige Datenerhebung informiert hatte wurde in Abstimmung mit mir am 21.09.2017 ein Runderlass veröffentlicht. Dieser informierte die Wohngeldstellen über die datenschutzrechtliche Unzulässigkeit des Vordrucks. Zudem wies der Erlass darauf hin, dass allenfalls im Rahmen einer Plausibilitätsprüfung anlassbezogen eine optionale Checkliste auf freiwilliger Basis verwendet werden kann.

# 6.3 Ohne Tadel: Prüfung der Gesundheitsregionen abgeschlossen

In meinem Tätigkeitsbericht für die Jahre 2015 und 2016 habe ich dargestellt, dass ich begonnen habe, die Gesundheitsregionen in Niedersachen datenschutzrechtlich zu überprüfen. Alle 35 zu diesem Zeitpunkt anerkannten Gesundheitsregionen wurden aufgefordert, mir die geplanten oder durchgeführten Projekte zur Verarbeitung von Gesundheitsdaten zu beschreiben. Die Prüfung konnte im ersten Halbjahr 2018 zufriedenstellend abgeschlossen werden.

Der Großteil der Gesundheitsregionen hat sich im Prüfzeitraum auf die Erstellung von Informationsmaterial und die Durchführung von Informationsveranstaltungen konzentriert. Drei Projekte waren jedoch von besonderer Bedeutung.

## Projekt „genial-Lotse“ des Landkreises Emsland

Bei diesem Projekt handelte es sich um eine Unterstützung für Patienten im erwerbsfähigen Alter, die sich im Genesungsprozess befanden. Hierfür stellte das Ärztenetzwerk Genial[1] den beteiligten Hausarztpraxen einen Lotsen zur Verfügung, der therapeutische Abläufe koordinieren und hemmende psychosoziale Faktoren erfassen sollte. In der Arbeit mit den Patienten sollte die Eigenmotivation und Selbstorganisation gestärkt werden. Ziel des Projektes war eine schnellere Genesung der Patienten. Von Vorteil für die Praxis sollte die Reduzierung von bürokratischen Vorgängen sein.

Die Erhebung und Verarbeitung der Gesundheitsdaten im Rahmen des Projektes durch den Lotsen und die Arztpraxen erfolgte auf Basis einer Einwilligung der Patientinnen und Patienten. Der Landkreis hat zu diesem Projekt ein schlüssiges Datenschutzkonzept vorgestellt.

Arztpraxen erhalten Lotsen

[1] Gesundheitsnetz im Altkreis Lingen eG

Positive Resonanz der Beteiligten

Der Projektzeitraum endete zum 31.12.2017 mit einer anonymen Befragung der Teilnehmenden. Aufgrund der positiven Resonanz aller Beteiligten soll das Projekt grundsätzlich weitergeführt werden. Eine Finanzierung ist derzeit jedoch noch nicht geklärt.

Datenschutzrechtlich war dieses Projekt nicht zu beanstanden. Weder bei den Verantwortlichen des Landkreises Emsland, noch bei meiner Behörde sind dazu datenschutzrechtliche Beschwerden eingegangen.

## Projekt „Wundnetz Emsland" des Landkreises Emsland

Ziel des Wundnetzes ist die Verbesserung der Versorgung von Patienten mit chronischen Wunden durch die Implementierung eines einheitlichen regionalen Versorgungskonzepts. Die Versorgung von Patienten mit chronischen Wunden wird in der Regel durch mehrere verschiedene Berufsgruppen – ärztliche und nichtärztliche – sowie in unterschiedlichen Settings – Haus- und Facharztpraxen, ggf. Krankenhaus, Praxen therapeutischer Berufsgruppen – wahrgenommen. Mit dem Zweck, die am Versorgungsprozess Beteiligten informationell zu vernetzen, wurde eine Datenbank entwickelt, in der alle relevanten Behandlungsdaten gespeichert werden und für die Beteiligten abrufbar sind.

Datenbank zur Vernetzung von Behandlern

In die Datenbank wurden nur Patienten mit ihren versorgungsbezogenen und medizinischen Daten aufgenommen, die zuvor schriftlich ihr Einverständnis erklärt hatten. Neben der individuellen Versorgung bestand auch die Möglichkeit, einer anonymisierten Nutzung der eigenen Daten zur Erstellung eines Leitfadens zur Diagnostik und Therapie zuzustimmen.

Auch bei diesem Projekt wurde der Datenschutz durch die Verantwortlichen sehr ernst genommen, sodass sich keine Beanstandungen oder Beschwerden von Betroffenen ergeben haben.

## Projekt „Erleben" von mehreren Landkreisen

Überlebensrate nach Herzstillstand steigern

Im Prüfzeitraum befand sich dieses Projekt noch in der Planungsphase. Ziel ist es, bei einem Herzstillstand die therapiefreie Zeit bis zum Eintreffen des Rettungsdienstes durch zufällig in der Nähe befindliche Ersthelfer zu verkürzen und dadurch die Reanimationsrate deutlich zu erhöhen. Hierzu sollte eine App entwickelt werden, mit Hilfe derer registrierte Nutzer, die über eine medizinische Schulung in der Herz-Lungen-Massage verfügen, über einem Notfall in unmittelbarer Nähe informiert werden.

Personenbezogene Gesundheitsdaten werden bei diesem Projekt nicht verarbeitet. Die Nutzenden erhalten nach Bestätigung, dass sie einen Rettungsversuch durchführen können, lediglich eine Information, an welchem Ort ein Notfall vorliegt. Auch die Daten der registrierten Ersthelfer werden in der App lediglich mit einem Pseudonym verarbeitet.

Datenschutzrechtlich ist dieses Projekt daher ebenfalls nicht zu beanstanden.

Innovation auch mit Datenschutz möglich

Eine Darstellung dieser Projekte ist mir wichtig, gerade weil in keinem Fall eine Beanstandung ausgesprochen werden musste. Die vorliegenden Fälle zeigen anschaulich, dass selbst im datenschutzrechtlich sensiblen Gesundheitsbereich innovative Projekte nach wie vor möglich sind, ohne gegen geltendes Recht zu verstoßen.

# 6.4 Anlassunabhängige Prüfung von Krankenhäusern

Der Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) zum 25. Mai 2018 hat auch den Datenschutz im Gesundheitsbereich maßgeblich beeinflusst. Die Sensibilität der Gesundheitsdaten wurde durch die DS-GVO noch einmal hervorgehoben. Grund genug, den Datenschutz in den Krankenhäusern genauer zu betrachten. Zu diesem Zweck habe ich eine anlassunabhängige Prüfung in drei Krankenhäusern begonnen, die sich in drei Fragenkomplexe gliedert.

## Datenschutzbeauftragte in den Kliniken

Die datenschutzrechtlichen Handlungsfelder in den Krankenhäusern sind vielfältig. Die betrieblichen Datenschutzbeauftragten vor Ort müssen die Einhaltung des Datenschutzes gegenüber den Beschäftigten genauso kontrollieren wie in Bezug auf die Patientinnen und Patienten. Dies setzt nicht nur umfangreiche Kenntnisse im Datenschutzrecht voraus, sondern auch ausreichende zeitliche Ressourcen bzw. eine ausreichende Anzahl an Beschäftigten, die den Datenschutzbeauftragten (nicht nur während des Urlaubs oder bei Abwesenheit) vertreten und unterstützen. Mein Augenmerk gilt daher der Frage, ob die Datenschutzbeauftragten ausreichend Zeit haben, ihre umfassenden Pflichten gewissenhaft erfüllen zu können.

Beauftragte benötigen ausreichend Zeit

## Orientierungshilfe zu Krankenhaus-Informationssystemen

Die datenschutzrechtlichen Regelungen im Gesundheitswesen waren in Deutschland bereits vor der DS-GVO auf einem sehr hohen Niveau. Für den Bereich der Krankenhäuser gibt es seit einigen Jahren bereits eine von den Datenschutzaufsichtsbehörden entwickelte Orientierungshilfe Krankenhaus-Informationssysteme, welche die rechtlichen Auslegungen der Aufsichtsbehörden zu den Datenschutzvorschriften enthält. Diese Orientierungshilfe behält auch mit der DS-GVO ihre Gültigkeit. Ein Kernpunkt meiner Prüfung sind die Zugriffsberechtigungen auf die Informationssysteme.

Orientierungshilfe – Kurzlink: https://t1p.de/Krankenhausinfosysteme

## Betroffenenrechte

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.

1 §§ 630a ff. BGB

Dennoch bringt die DS-GVO auch in diesem Bereich Neuerungen mit sich. Wie in allen anderen Bereichen sind auch die Patienten eines Krankenhauses vor Beginn der Verarbeitung ihrer personenbezogenen Daten über die Art und Weise der Datenverarbeitung zu informieren.

DS-GVO sieht Informationspflichten vor

Die Umsetzung des Auskunftsrechts nach der DS-GVO und der Informationspflichten sind ebenfalls Bestandteil der Prüfung.

Der Abschluss der Prüfung ist für den Sommer 2019 vorgesehen. Ergebnisse werden in meinem folgenden Tätigkeitsbericht präsentiert.

# 6.5 Juristisches Kompetenzzentrum im Maßregelvollzug:

## Im zweiten Anlauf datenschutzgerecht

Durch einen Erlass des Ministeriums für Soziales, Gesundheit und Gleichstellung (MS) vom 21.2.2017 erfuhr ich, dass die Einrichtung eines juristischen Kompetenzzentrums im Maßregelvollzug (JZM) beschlossen worden war. Dieses soll die Vollzugsleitungen bei einer Entscheidung, ob die Vollzugsbedingungen für Patienten gelockert werden, juristisch beraten und unterstützen. Zunächst wurde es jedoch versäumt, eine entsprechende Rechtsgrundlage für die Übermittlung der Patientendaten an das Kompetenzzentrum zu schaffen.

Weitere Kontrollinstanz nachvollziehbar

Maßregelvollzugseinrichtungen sind geschlossene Krankenhäuser. In ihnen werden psychisch kranke Straftäter untergebracht, bei denen eine weitere Gefährdung für die Allgemeinheit zu erwarten ist.

Aufgrund einiger Vorfälle, in denen Patienten die gewährten Vollzugslockerungen zur Flucht und Verübung weiterer Rechtsbrüche genutzt haben, ist die Errichtung einer weiteren Beratungs- und Kontrollinstanz in Form des JZM nachvollziehbar und zu begrüßen.

Aufgabe des JZM soll jedoch nicht nur eine allgemeine Beratung zu verschiedenen Sachverhalten sein, sondern auch die juristische Prüfung des konkreten Einzelfalls. Hierzu ist es erforderlich, dass das JZM vor Gewährung einer Vollzugslockerung die gesamten Akten (Straf- und Gesundheitsakten) eines Untergebrachten prüft.

## Keine Rechtsgrundlage für die Datenübermittlung

Für die Verarbeitung von Gesundheitsdaten war auch vor Geltung der Datenschutz-Grundverordnung (DS-GVO) eine konkrete Rechtsgrundlage erforderlich. Ein Erlass wirkt jedoch nur verwaltungsintern und stellt keine entsprechende Rechtsgrundlage dar. Das Niedersächsische Maßregelvollzugsgesetz enthielt keine derartige Befugnisnorm.

Übermittlung nur mit Einwilligung möglich

Ohne eine gesetzliche Übermittlungsgrundlage dürfen personenbezogene Daten nur mit Einwilligung der betroffenen Person an Dritte übermittelt werden. Ich habe das MS daher im Juni 2017 aufgefordert, umgehend eine entsprechende Rechtsänderung einzuleiten.

## Einwilligung muss freiwillig sein

Dies war umso wichtiger, da die Einwilligung in diesem Fall offensichtlich nicht das geeignete Mittel war. So entschied das Landgericht Göttingen am 6.11.2017 über einen Fall, in welchem einer im Maßregelvollzug untergebrachten Person ein Antrag auf Vollzugslockerung abgelehnt worden war. Grund: Sie hatte nicht ihr Einverständnis in die Datenübermittlung an das JZM erteilen wollen. Ein Hauptbestandteil einer wirksamen Einwilligung ist deren Freiwilligkeit. Inwieweit eine Freiwilligkeit bei einer im Maßregelvollzug untergebrachten Person überhaupt gegeben sein kann, ist bereits fraglich. Die Ablehnung eines Antrags darf jedoch keinesfalls allein von einer freiwilligen Einwilligung abhängig gemacht werden. Entsprechend gab das Landgericht dem Antrag des Beschwerdeführers statt[1].

Neue Vorschrift ins Gesetz eingefügt

Im Rahmen des Artikels 14 des Gesetzes zur Neuordnung des niedersächsischen Datenschutzrechts[2] wurde im Maßregelvollzugsgesetz zum 25. Mai 2018 eine Vorschrift eingefügt, welche es Stellen erlaubt, Gesundheitsdaten zur Erfüllung ihrer Aufgaben verarbeiten zu dürfen[3]. Die Einbindung des JZM erfolgt nun in rechtlich zulässiger Weise.

1 Landgericht Göttingen, Beschluss vom 06.11.2017 – 53 StVK 91/17

2 Nds. GVBl. Nr, 6/2018

3 § 21b Nds. MVollzG

# 6.6 Schulzahnärztliche Untersuchungen – Kinder haben Anspruch auf Datenschutz

Die Zahngesundheitspflege ist eine gesetzliche Aufgabe, die bei der schulzahnärztlichen Untersuchung wahrgenommen wird – in der Regel durch die Gesundheitsämter. Hierzu gibt es in Niedersachsen aufgrund des kommunalen Selbstverwaltungsrechts zahlreiche verschiedene Informationsbroschüren, Einwilligungserklärungen und Verfahren. Ein datenschutzgerechtes Muster gab es bislang nicht, was immer wieder zu Beschwerden führte.

Arbeitsgruppe entwirft datenschutzkonformes Muster

Um Abhilfe zu schaffen, habe ich eine datenschutzgerechte Vorgehensweise erstellt und mich mit dem Ministerium für Soziales, Gesundheit und Gleichstellung (MS) in Verbindung gesetzt, damit dieses als Fachaufsicht über die Gesundheitsämter eine entsprechende Arbeitsanweisung erlässt. Daraufhin wurde kurzfristig mit dem MS, dem Niedersächsischen Landesgesundheitsamt (NLGA) und meiner Behörde eine Arbeitsgruppe gegründet. Diese erstellte neben meinen Arbeitsanweisungen ein einheitliches, datenschutzgerechtes Muster für die Information der Eltern, die Einwilligung und den Verfahrensablauf.

## Besondere Brisanz bei Kindern und Jugendlichen

Medizinische Daten unterliegen einem besonderen Schutz. Noch brisanter werden Datenschutzverstöße im vorliegenden Fall durch die Tatsache, dass hier Kinder und Jugendliche betroffen sind. Da nun ein mit allen Beteiligten abgestimmtes, datenschutzkonformes Muster beim NLGA zur Verfügung steht, empfehle ich allen Kommunen, sich eng daran zu orientieren.

# 6.7 Datenaustausch zwischen Kita und Jugendamt auch ohne Einwilligung der Eltern zulässig

Nicht in allen Fällen, in denen das Personal einer Kindertagesstätte (Kita) personenbezogene Daten des Kindes und seiner Eltern verarbeitet, muss es deren Einwilligung einholen. Im vorliegenden Fall durfte die Kita Daten an die Kita-Fachberatung des Jugendamtes ohne Einwilligung übermitteln, um Aufsichts- und Kontrollaufgaben wahrzunehmen.

Die Mitarbeiter einer kommunalen Kita wollten mit den Eltern eines Kindes ein informierendes Gespräch führen. Sie hatten dazu im Vorfeld die Kita-Fachberatung, die dem Jugendamt angegliedert ist, informiert und dabei auch personenbezogene Daten über das Kind und seine Eltern ausgetauscht. Im Ergebnis vereinbarten sie, dass neben dem Kita-Personal auch eine Mitarbeiterin der Fachberatung beim Gespräch anwesend sein sollte. Die Eltern sahen durch diesen Austausch und die Anwesenheit einer weiteren Person, die nicht dem Kita-Personal angehört, den Sozialdatenschutz verletzt, da sie nicht um ihre Einwilligung gebeten worden waren.

## Fachberatung nimmt auch Aufsicht wahr

Im Gespräch mit der Fachberatung und dem Datenschutzbeauftragten des Jugendamtes stellte sich heraus, dass die Fachberatung des Jugendamtes neben ihren ursächlichen Aufgaben wie z. B. Qualitätssicherung und -entwicklung in Kitas oder Organisation von Fort- und Weiterbildungen auch Aufgaben der Fachaufsicht wahrnimmt. In diesem Zusammenhang wird sie beispielsweise für fachliche Hilfe bei Problemen in einer Kita angefragt. Um einen solchen Fall handelte es sich hier. Für die Beratung im Rahmen der Fachaufsicht war es notwendig, der Fachberatung personenbezogene Daten mitzuteilen.

Austausch der Daten war notwendig

## Datenschutzbeauftragter der Kita kann meist helfen

Rechtsgrundlage hierfür ist § 67c Abs. 3 Zehntes Buch Sozialgesetzbuch. Danach dürfen für Aufsichts- und Kontrollaufgaben personenbezogene Daten ohne Einwilligung der Eltern weitergegeben werden. Das Handeln der Kita war daher datenschutzrechtlich nicht zu beanstanden. Ich habe die Eltern und die Kita entsprechend informiert.

Kita hat datenschutzkonform gehandelt

Generell empfehle ich Eltern bei Fragen zur Datenverarbeitung der Kita, sich als erstes an den Datenschutzbeauftragten der Tagesstätte zu wenden. Dieser kennt die Gegebenheiten vor Ort und kann in der Regel umfassend Auskunft geben.

# F.7. Datenschutz in der Wirtschaft

## 7.1 Prüfung zur Umsetzung der DS-GVO in 50 niedersächsischen Unternehmen

In einer branchenübergreifenden Querschnittsprüfung schrieb ich Ende Juni 2018 50 große und mittelgroße Unternehmen mit Hauptsitz in Niedersachsen an. Sie sollten Fragen zu zehn Bereichen des Datenschutzes beantworten. Ziel dieser bislang größten Prüfung in der Geschichte meiner Behörde ist es, einen Überblick darüber zu erhalten, wie die Firmen die zweijährige Übergangszeit bis zur Geltung der Datenschutz-Grundverordnung (DS-GVO) genutzt haben.

Aufklärung geht vor Sanktion

Das Hauptanliegen der Prüfung ist es zu identifizieren, ob und in welchen Bereichen es bei den verantwortlichen Stellen noch Nachholbedarf gibt. Außerdem möchte ich mit dieser Prüfung das Bewusstsein für den Datenschutz im Allgemeinen und für die Vorschriften der DS-GVO im Speziellen stärken. Es geht nicht vorrangig darum, möglichst viele Fehler zu finden und Bußgelder zu verhängen. Stattdessen wollen wir aufklären, sensibilisieren und wertvolle Hinweise geben. Trotzdem sind natürlich weiterführende Verfahren nicht ausgeschlossen, sollten während der Prüfung erhebliche Verstöße gegen die DS-GVO festgestellt werden.

Konsequenzen für Arbeit der LfD

Ich erhoffe mir darüber hinaus auch Hinweise für die zukünftige Arbeit meiner Behörde. So könnten sich zum Beispiel Schwerpunktprüfungen zu bestimmten Themen oder in bestimmten Branchen anschließen. Außerdem erwarte ich Anhaltspunkte dafür, wo noch besonders viel Beratungs- und Aufklärungsbedarf besteht.

### Offene Fragen statt Multiple Choice

Den Fragebogen haben zunächst 20 große und 30 mittelgroße Unternehmen aus verschiedenen Branchen erhalten, die ihren Hauptsitz in Niedersachsen haben. Die Fragen, die auf der „Checkliste für die Umstellung kleinerer Unternehmen auf die Datenschutz-Grundverordnung“ basieren, welche ich im November 2017 veröffentlicht habe, waren bewusst offen gewählt worden,

um den Unternehmen die Möglichkeit zu bieten, ihre Antworten auf ihre konkrete Situation/Größe anzupassen. Gleichzeitig möchte ich einen Hinweis darüber erhalten, wie weit die einzelnen Anforderungen der DS-GVO bei den Unternehmen bereits erkannt und prozessual umgesetzt wurden. Mit einem Multiple-Choice-Bogen wäre das nicht möglich.

Abschlussbericht im Mai 2019

Im vierten Quartal 2018 haben meine Mitarbeiterinnen und Mitarbeiter mit der Auswertung der Antworten begonnen und werden diese Ende Januar 2019 abschließen. Anschließend werden bei ausgewählten Unternehmen Vor-Ort-Termine zur Verifizierung und Vertiefung durchgeführt. Der Abschlussbericht der Querschnittsprüfung soll dann im Mai 2019 vorliegen.

Ich werde in meinem nächsten Tätigkeitsbericht ausführlich über Ablauf, Ergebnisse und Folgen dieser Prüfung berichten.

# 7.2 Musteranleitung für das vernetzte Auto

Freiwilligkeit setzt Wahlmöglichkeiten und Transparenz voraus – auch beim Datenschutz im Auto. In einer Gemeinsamen Erklärung mit der Automobilindustrie haben die Datenschutzbehörden als verbindliches Ziel ausgegeben, dass in jeder Borddokumentation transparent nachlesbar sein soll, was das Auto eigentlich mit Ihren Daten macht.

Gemeinsame Erklärung mit dem VDA

In meinem Tätigkeitsbericht 2015/2016 habe ich über die Gemeinsame Erklärung der Datenschutzbehörden des Bundes und der Länder mit dem Verband der Automobilindustrie (VDA) berichtet. Darin wurde erstmals der Rahmen für den Datenschutz im Auto festgelegt. Im Zeitraum für den vorliegenden Bericht ging es nun darum, die Inhalte der Erklärung in die Tat umzusetzen. So haben die Datenschutzaufsichtsbehörden mit dem VDA ein Musterkapitel „Datenschutz“ für die Betriebsanleitung im Autocockpit erarbeitet. Dieses soll in sämtlichen Kfz etlicher deutscher Hersteller Verwendung finden – markenübergreifend.

## Zentral, verständlich, einheitlich

Schon die Existenz des Mustertextes stellt einen wichtigen Baustein für Transparenz dar. Denn bislang waren Ausführungen zum Datenschutz für Autofahrer oft an vielen verschiedenen Stellen zu finden. Das einheitliche Musterkapitel ermöglicht es, die wichtigsten Informationen an nur einer zentralen Stelle aufzuführen. Zudem kommunizieren die Hersteller so einheitlich und in sachlicher, verständlicher Sprache mit den Betroffenen. Nicht zuletzt ist auch eine einheitliche Begrifflichkeit – jenseits formeller Gesetzesformulierungen – wichtig, um Datenverarbeitungen erkennen und unterbinden zu können. All das wird mit dem Musterkapitel Datenschutz ermöglicht.

Verarbeitungen erkennen und unterbinden können

Das Musterkapitel gibt die in der Gemeinsamen Erklärung vereinbarten Inhalte für jeden Autofahrer wieder und sorgt damit dafür, dass keiner der beteiligten Hersteller hinter den verbindlich vereinbarten Standard zurückfallen kann.

Das Musterkapitel enthält folgende Teile:

- „Personenbezug“
- „Ihre Rechte im Hinblick auf den Datenschutz“
- „Gesetzliche Anforderungen zur Offenlegung von Daten“
- „Betriebsdaten im Fahrzeug“
- „Online-Dienste“
- „Herstellereigene Dienste“
- „Dienste Dritter“.

## Es gibt keine rein technischen Daten

Der Abschnitt „Personenbezug“ hält ganz zu Beginn fest, dass alle von Steuergeräten generierten bzw. verarbeiteten Daten personenbezogen sein können. Damit wird der zentrale Punkt der schon Gemeinsamen Erklärung umgesetzt: dass alle bei der Kfz-Nutzung anfallenden Daten dann personenbezogen im Sinne der Datenschutzgesetze sind, wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt. Es gibt also keine rein technischen Daten, die Datenschutzgesetze finden grundsätzlich immer Anwendung. Das kann nun nachgelesen werden – quasi in jedem Auto.

Prägnante Information der Betroffenen

Wichtig für das Musterkapitel war vor allem, dass der Betroffene prägnant informiert wird, welche hauptsächlichen Kategorien der Datenverwendung im Kfz es überhaupt gibt. Beim Auslesen sämtlicher Fahrzeugdaten ergeben sich in der Regel abertausende Datenzeilen. Das kann kein Laie überschauen. Also war es das Ziel, die wesentlichen, übergreifenden Kriterien der Datenverwendungen in wenigen Absätzen zusammenzufassen. Der Betroffene sollte auf einen Blick unterscheiden können: zwischen für das Fahren erforderlichen Datenverwendungen, einschließlich Fehlerdiagnosen, und freiwilligen Zusatzfunktionen wie z.B. Infotainment-Datenverwendungen.

## Auch Gelegenheitsfahrer müssen sich informieren können

Bewusste Entscheidung nur mit Transparenz

Um diese Entscheidung zwischen für das Fahren notwendigen und nicht notwendigen Verwendungen treffen zu können, muss der betroffene Fahrer transparent informiert werden. Denn nur bei voller Transparenz können die Betroffenen bewusste Entscheidungen darüber treffen, welchen Datenverarbeitungen sie in aufgeklärter Weise zustimmen. Das gilt zum einen für Betroffene, die direkt vom Hersteller ein Auto kaufen. Transparenz ist aber ebenso wichtig für Zweitkäufer und für weitere Fahrer (z.B. Familienmitglieder; Freunde), die das Auto für einzelne Fahrten vom Besitzer ausborgen.

Die größte Herausforderung bei der Erstellung des Musterkapitels war es, den Text möglichst kurz zu halten. Denn ein transparenter Überblick ist nur möglich, wenn die Information auf wenige Seiten passt. Das ist uns gelungen und die beteiligten Hersteller können nun das Musterkapitel auf verschiedene Weise verwenden: etwa als elektronisch abrufbaren Text im Cockpit oder als Teil der gedruckten Betriebsanleitung.

# 7.3 Schwerpunktprüfung in Kfz-Werkstätten

Kfz-Werkstätten wechseln nicht nur Reifen, Öl oder Luftfilter. Häufig ist es auch nötig, Daten aus dem Auto auszulesen. Über die konkrete Art dieser Datenerhebungen habe ich mir im Rahmen einer Schwerpunktprüfung ein Bild gemacht. Das Ergebnis war erfreulich.

Im Jahr 2017 habe ich zusammen mit den Aufsichtsbehörden aus Bayern, Baden-Württemberg, Brandenburg, Hessen und Nordrhein-Westfalen, eine Prüfung von Kfz-Werkstätten durchgeführt. In deren Rahmen habe ich in Nie-

dersachsen zehn Werkstätten geprüft. In die Auswahl einbezogen wurden sowohl kleine selbständige („freie“) Werkstätten als auch größere, markenübergreifende sowie markengebundene Vertragswerkstätten. Nennenswerte Verstöße habe ich bei den von mir geprüften Werkstätten nicht feststellen können.

Keine nennenswerten Verstöße

Ziel der Prüfung war es, die konkreten Abläufe etwaiger Datenerhebungen in den Werkstätten zu beleuchten und zugleich abzufragen, auf welche Rechtsgrundlage die Datenverarbeitungen gestützt werden. Zunächst ging es also um die Frage, ob die Werkstätten bei Wartung bzw. Reparatur Daten aus dem Fahrzeug in ihren Systemen speichert – und wenn ja, welche?

## Datenerhebung an konkreten Auftrag geknüpft

Das Auslesen von Daten beim Werkstattaufenthalt ist in der Regel eng mit dem konkreten Auftrag verbunden. Die Prüfung ergab, dass - sofern es für die Wartung bzw. Reparatur erforderlich ist - insbesondere die Fahrzeugidentifikationsnummer (FIN), der Kilometerstand, Verbrauchswerte, abgasrelevante Informationen und Fehlercodes ausgelesen werden. Die geprüften Werkstätten waren sich bewusst, dass der Umfang der Datenerhebung an den konkreten Reparaturauftrag geknüpft ist. Sofern eine elektronische Erhebung nicht geboten war, wurden die Daten teilweise auch handschriftlich erhoben (insbesondere Name des Kunden, Fahrzeugtyp, Kfz-Kennzeichen, FIN, Auftragsbeschreibung).

Erhebung zum Teil handschriftlich

Zu Recht gingen die Werkstätten mehrheitlich davon aus, dass für den Werkstattaufenthalt zwingend erforderliche Daten die Rechtsgrundlage für die Datenverarbeitung bereits aus dem Werkstattvertrag folgt. Da diese Daten ausgelesen werden müssen, um den Vertrag zu erfüllen, besteht also bereits eine gesetzliche Grundlage für die Datenverwendung. Deshalb ist keine zusätzliche Einwilligung der Kunden nötig.

## Einwilligung muss zweckgebunden sein

Dennoch wurde von einigen Werkstätten fälschlicherweise angenommen, dass sie trotzdem eine Einwilligung einholen müssten. Diese wäre aber nicht nur überflüssig. Die bundesländerübergreifende Auswertung der Prüfung ergab auch, dass sie teilweise zu weitgehend formuliert war, nämlich als pauschale Einwilligung „in die Verarbeitung Ihrer Daten“. Sofern eine Einwilligung überhaupt erforderlich wäre, muss sie aber zweckgebunden sein, d.h., es muss ersichtlich sein, welche Daten auf welche Weise und zu welchem Zweck verarbeitet werden.

Ein weiterer Schwerpunkt der gemeinsamen Prüfung war, ob die Kunden von der Datenverarbeitung transparent in Kenntnis gesetzt wurden. Die Prüfung ergab, dass die Werkstätten teilweise davon ausgingen, dieser Anforderung sei mit der Betriebsanleitung des jeweiligen Kfz-Herstellers Genüge geleistet. Damit kommt eine Werkstatt ihren Informationspflichten allerdings nicht nach. Wird ein Werkstattauftrag erteilt, muss die Werkstatt selbst über die Datenverarbeitung informieren. Hierfür kommt etwa ein Informationsblatt in Betracht.

Werkstätten haben Informationspflicht

# 7.4 Datenweitergabe an Bezahldienst ohne Zustimmung

Der Bezahldienst Paydirekt ging im August 2015 unter Beteiligung von 40 Banken in die Pilotphase. Mit dabei waren sowohl private Finanzhäuser als auch die Genossenschaftsbanken sowie die Sparkassen. Den Kreditunternehmen ging es um eine deutsche (europäische) Entwicklung als Konkurrenz zum weltweit führenden Online-Bezahldienst PayPal. Einige Kunden fragten bei mir an, ob ohne ihre explizite Zustimmung die Weiterleitung der Daten an einen Zahlungsdienstleister zulässig sei.

## Schweigen bedeutet Zustimmung

Per Mitteilung wurden die Bankkunden über das neue Bezahlverfahren informiert. Darin boten die Banken an, die Anmeldung für ihre Kunden vorzubereiten und zu vereinfachen. „Wenn Sie damit einverstanden sind, brauchen Sie nichts weiter unternehmen“, hieß es weiter. „Dann gehen wir von Ihrer Zustimmung aus und leiten Ihre Daten an unseren technischen Zahlungsdienstleister - die paydirekt GmbH - zur Registrierung weiter.“

Außerdem wurde dem Kunden auch die Möglichkeit angeboten, zu widersprechen, falls er den Service nicht wünschte. Die Daten würden dann nicht weitergeleitet. Der Widerspruch habe zudem keine Auswirkungen auf den bestehenden Girokontovertrag.

Widerspruch ohne Folgen für das Girokonto

Weitere Hinweise und Informationen zur Nutzung von Paydirekt gaben die Banken durch beigefügte Anlagen, Internetseiten und ggf. telefonisch.

## Opt out in diesem Fall zulässig

Aus datenschutzrechtlicher Sicht war die Weiterleitung der Daten ohne Aktivierung durch den Kunden zulässig, wenn kein Widerspruch eingelegt wurde. Im Unterschied zu anderen Bezahldiensten ist Paydirekt kein Drittanbieter, sondern eine Zusatzfunktion des Girokontos. Es besteht kein Vertragsverhältnis des Kunden zur paydirekt GmbH. Die Firma, ein Gemeinschaftsunternehmen der Deutschen Kreditwirtschaft, ist lediglich technischer Dienstleister der Kreditinstitute, der im Rahmen eines Geschäftsbesorgungsvertrags tätig ist.

Kein Vertrag zwischen Kunde und Paydirekt

Die Zahlung wird direkt über das Girokonto des Käufers abgewickelt und an das Konto des Händlers gesendet. Die Konto-Informationen werden dabei weder an den Händler noch an einen Drittanbieter weitergegeben. Aufgrund der zivilrechtlichen Regelung des § 675g Abs. 1 und Abs. 2 BGB sowie der jeweiligen AGB-Bestimmungen kann ein Kreditinstitut einseitig eine Vertragsänderung unter bestimmten Voraussetzungen gegenüber dem Kunden durchführen (Zustimmungsfiktion). Deshalb ist in diesem Fall ein Opt-out-Verfahren gesetzlich zulässig. Der Kunde wird auf sein Widerspruchs- bzw. Kündigungsrecht hingewiesen. Der bisher geltende Vertrag wird im Falle des Widerspruchs unverändert fortgeführt.

# 7.5 Datenübermittlung bei Online-Überweisungen

Welche Daten dürfen im Zahlungsverkehr von einer Bank übertragen werden? Einige Bankkunden fragten bei mir an, ob es zulässig sei, dass vom Kreditinstitut bei jeder Online-Überweisung die IBAN des Zahlers an den Empfänger übertragen wird. Die Weiterleitung der Kundenkennung des Zahlers ist seit 2011 immer wieder Gegenstand von datenschutzrechtlichen Diskussionen gewesen.

## Unterschiedliche Auffassungen bei Kreditwirtschaft und Datenschützern

Banken: IBAN muss mitgeteilt werden

Nach Auffassung der Kreditwirtschaft ist die Weiterleitung mit dem Datenschutzrecht vereinbar. Sie argumentiert, die Bank des Zahlungsempfängers an diesen alles weiterleiten muss bzw. kann, was sie selbst erhalten hat, nämlich den Zahlungsbetrag und alle Auftragsdaten (Gebot der formalen Auftragsstrenge). Dabei berufen sich die Geldinstitute auf Art. 248 § 8 Nr. 1 EGBGB und § 675r BGB für die Übermittlung der IBAN an Überweisungsempfänger. Der Wortlaut dieser Vorschriften ist recht eindeutig. Danach müssen dem Empfänger „alle weiteren mit dem Zahlungsvorgang übermittelten Angaben" mitgeteilt werden. Dazu gehört dann auch die IBAN. Insoweit können sich die Banken auf Art. 6 Abs. 1 lit c) DS-GVO stützen. Dieser besagt, dass die Verarbeitung von Daten rechtmäßig ist, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

Datenschützer verweisen auf Sparsamkeit

Einige Datenschutzaufsichtsbehörden haben Zweifel an dieser Rechtsauffassung und verweisen auf die grundsätzlichen Regelungen der DS-GVO zur Datensparsamkeit und Erforderlichkeit einer Datenübermittlung – so auch ich. Diese Auffassung wird gestützt durch Erwägungsgrund 54 der 2. Zahlungsdiensterichtlinie. Darin steht, dass der Name des Zahlenden und der Verwendungszweck als „notwendige" Information ausreichend wären. Im Einzelfall könnte aber auch die IBAN eine notwendige Information sein. Etwa dann, wenn sie im Fall eines falsch oder zu viel überwiesenen Betrages dazu dient, eine Rücküberweisung zu veranlassen.

## Keine Rechtsgrundlage für Anordnung

Empfehlung: auf IBAN verzichten

Da die Datenübermittlung nicht unzulässig ist, besteht für eine entsprechende Anordnung durch die Datenschutzaufsichtsbehörde allerdings keine Rechtsgrundlage. Im Sinne der Datenminimierung und des vertrauensvollen Umgangs mit Kundendaten kann ich Banken allerdings nur raten, eine Übermittlung der IBAN an den Zahlungsempfänger zu hinterfragen und bestenfalls darauf zu verzichten. Ich werde diese Rechtsdiskussion weiterhin eng begleiten.

# 7.6 Personalausweiskopie jetzt möglich

Zuletzt hatte ich das Kopieren und Speichern von Personalausweisen im Tätigkeitsbericht 2013-2014 thematisiert. Mit Änderung des Personalausweisgesetzes haben sich auch die rechtlichen Regelungen für das Kopieren, Fotografieren und Scannen von Personalausweisen geändert. Der Ausweis darf nun unter bestimmten Voraussetzungen auch abgelichtet und die darin enthaltenen personenbezogenen Daten dürfen verarbeitet werden.

Immer wieder kommt es im Alltag zu Situationen, in denen um Übergabe des Personalausweises gebeten wird, zum Beispiel als „Sicherheit" bei der Autovermietung. Das dient meist nicht nur der Feststellung der Identität. Oft wird auch eine Kopie oder sogar ein Scan des Ausweises angefertigt.

Scan war bisher verboten

Dies führte bei mir immer wieder zu Eingaben und Beschwerden. In der Vergangenheit zu Recht, denn besonders das Einscannen und damit Speichern war bisher grundsätzlich verboten, was durch ein Grundsatzurteil des Verwaltungsgerichts Hannover 2013 bestätigt wurde.

Der Gesetzesgeber hat das Personalausweisgesetz im Juli 2017 geändert. Neu ist, dass der Ausweis nun auch „abgelichtet" werden darf.
Der abstrakte Begriff des Ablichtens umfasst die Handlungen Fotokopieren, Fotografieren und Einscannen.

Das Ablichten ist jedoch nur zulässig, sofern folgende Voraussetzungen vorliegen:

1. Nur der Ausweisinhaber (oder eine andere Person mit der Zustimmung des Ausweisinhabers) darf die Ablichtung vornehmen.

2. Die Ablichtung muss eindeutig und dauerhaft als Kopie erkennbar sein.

Kopie muss als solche erkennbar sein

Die Erkennbarkeit als Kopie lässt sich beispielsweise dadurch erreichen, dass sie in Monochromstufen (z. B. schwarz-weiß) erstellt oder nachträglich dauerhaft darauf umgestellt wird. Eine andere Möglichkeit besteht darin, auf der Fotokopie den deutlich sichtbaren Vermerk „Kopie" anzubringen.

Die Ablichtung kann wie folgt verwendet werden:

1. Nur der Ausweisinhaber darf die Kopie weitergeben.

2. Sofern personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet werden, darf dies nur mit Einwilligung des Ausweisinhabers geschehen.

## Handlungsempfehlungen:

Wenn eine verantwortliche Stelle den Personalausweis kopieren möchte, sollte sie Folgendes beachten:

Schwärzen, was nicht nötig ist

- Sie muss prüfen, ob das Erstellen einer Kopie wirklich erforderlich ist. Denkbar ist auch eine Notiz, dass der Ausweis vorgelegt wurde. Dies berücksichtigt den Grundsatz der Datenminimierung.
- Daten, die nicht erforderlich sind, müssen geschwärzt werden.
- Vor der Verarbeitung personenbezogener Daten aus dem Personalausweis durch Ablichtung muss eine Einwilligung des Ausweisinhabers vorliegen, die den Anforderungen der Datenschutz-Grundverordnung entspricht.
- Der Verantwortliche muss die Einwilligung im Rahmen der Rechenschaftspflicht nachweisen können.
- Werden die personenbezogenen Daten aus dem Personalausweis verarbeitet, muss der Verantwortliche den Ausweisinhaber gem. Art. 13 und 14 DS-GVO informieren.[1]
- Die gesetzlichen Speicherfristen müssen beachtet werden.

FAQ Informationspflichten: https://lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/faq/informationspflichten/informationspflichten-170998.html

# 7.7 Werbung als Polster trotz Widerspruch

Ein Unternehmen verschickte an Kunden Werbung für eigene Produkte im Zusammenhang mit Warensendungen, Rechnungen oder sonstigen Korrespondenzen. Es unterschied dabei nicht, ob die betroffenen Kunden einen Werbewiderspruch eingelegt hatten oder nicht. Mich erreichten dazu mehrere Beschwerden.

Werbung als Schutz vor Diebstahl?

Das Unternehmen argumentierte damit, dass es hochwertige und teure Waren versende würden, die für den Transport sicher geschützt und verpackt werden müssten. Es sei in der Vergangenheit beim Postversand immer wieder zu Diebstählen gekommen, weil sich der Inhalt der Sendung abgezeichnet habe oder ertastet werden konnte. Daher habe man sich entschlossen, zum Auspolstern der Warensendungen Werbematerial zu nutzen. Für den Kunden sollte es nach Ansicht des Versenders keine Rolle spielen, ob als zusätzliche Verpackung und Diebstahlschutz bedrucktes oder unbedrucktes Papier verwendet würde.

Werbung aus technischen Gründen?

Ähnlich wurde in Bezug auf Rechnungen oder sonstige Korrespondenz argumentiert. Hier sei aus drucktechnischen Gründen freier Platz nicht weiß geblieben, sondern für Werbemaßnahmen genutzt worden. Der Kunde würde keine zusätzliche Post bekommen. Es würden nur die erforderlichen und zulässigen Kundenkontakte um Werbeaufdrucke ergänzt. Dem Kunden würde dadurch auch kein Mehr an Papier zugemutet. Diese Vorgehensweise sei daher datenschutzrechtlich nicht zu beanstanden.

## Werbewiderspruch ist immer zu beachten

Verbindung mit zulässigem Kundenkontakt spielt keine Rolle

Dieser Auffassung konnte ich mich nicht anschließen. Für die datenschutzrechtliche Einordnung der Werbung spielt es keine Rolle, dass sie von Seiten des Unternehmens mit einem zulässigen Kundenkontakt, wie z. B. einer Zusendung bestellter Ware, verbunden wird. Es ist nicht sachgerecht, die beiden Aspekte - zulässiger Kundenkontakt auf der einen und durch Widerspruch unzulässige Werbung auf der anderen Seite - gleich zu behandeln, nur weil sie gemeinsam in einer Postsendung verschickt werden. Eine an sich unzulässige Werbung bleibt auch dann unzulässig, wenn sie mit einem zulässigen Kundenkontakt verbunden wird. Andernfalls bestünde die Gefahr, dass die Regelungen des Bundesdatenschutzgesetzes.[1] Umgangen werden.

Unternehmen stellt Abläufe um

Die fraglichen Werbemaßnahmen liegen nicht im Rahmen der vertraglichen Erforderlichkeit. Es handelt sich um zwei nach ihrem Zweck unterschiedliche und ohne weiteres voneinander trennbare Sachverhalte. Es ist daher datenschutzrechtlich unzulässig, Werbung zu Lieferungen, Rechnungen und/oder Freiflächen in sonstiger Korrespondenz an Kunden beizufügen, die Werbewiderspruch erhoben haben. Ich habe daraufhin das betroffene Unternehmen angewiesen, seine Praxis umzustellen. Das Unternehmen hat sich unserer Rechtsauffassung angeschlossen und mitgeteilt, die internen Abläufe entsprechend anzupassen. Der Vollzug der Anpassungen wurde uns anschließend schriftlich bestätigt.

1 s. auch Beschluss des OVG Berlin-Brandenburg vom 31.07.2015, Az.: OVG 12 N 71.14

# 7.8 Weitergabe von E-Mail-Adressen zur Sendungsverfolgung

Beim Online-Shopping kann der Kunde heutzutage nach dem Kauf den Weg des Produkts genau verfolgen und weiß so, wann die Sendung ankommt. Häufig übermittelt der Online-Händler dafür die E-Mail-Adresse des Käufers an den Postdienstleister. In diese Weitergabe muss der Kunde allerdings vorher eingewilligt haben. Dazu erreichen mich immer wieder Anfragen und Beschwerden.

Der Handel im Internet boomt. Mit wenigen Klicks ist die Ware bestellt und auf dem Weg zum Kunden. Um diesen darüber zu informieren, wo sich das gekaufte Produkt gerade befindet und wann es eintrifft, versenden viele Internet-Händler sogenannte Tracking-Mails. Allerdings kommen diese oft nicht vom Händler selbst, sondern direkt vom Paketdienst, dem der Shop-Betreiber die E-Mail-Adresse des Kunden übermittelt hat.

Tracking-Mails vom Zusteller

## Interessen des Kunden überwiegen

In der Datenschutz-Grundverordnung findet sich für diese Übermittlung der E-Mail-Adresse keine Rechtsgrundlage. Die Weitergabe an den Postdienstleister ist auch nicht zur Erfüllung eines Vertrags bzw. Schuldverhältnisses notwendig. Einem möglichen Interesse des Online-Händlers stehen die überwiegenden Interessen seiner Kunden entgegen, dass ihre E-Mail-Adressen nicht ohne Einwilligung an einen ihnen vorher unbekannten Postdienstleister übermittelt werden.

Somit ist die Übermittlung von E-Mail-Adressen durch Online-Händler an Postdienstleister nur rechtmäßig, wenn eine Einwilligung des Kunden vorliegt. Diese muss der Kunde mittels Opt-In erteilen. In diesem Fall setzt er z. B. aktiv ein Häkchen und stimmt zu, dass seine E-Mail-Adresse an einen Zustelldienst weitergegeben wird, um das Paket anzukündigen. Dabei sollten die Paketdienstleister namentlich benannt werden. Die Einwilligung wird somit informiert bei jeder Bestellung durch den Kunden erteilt.

Informierte Einwilligung per Opt-In

## Es geht auch ohne Weitergabe der Adresse

Statt die Mail-Adresse an den Postzusteller weiterzugeben, kann ein Shop-Betreiber alternativ die Zustellinformationen auch selbst an den Kunden weitergeben oder einen Link zur Sendungsverfolgung in die eigene Bestellbestätigung einbinden. In diesem Fall gelangt der Kunde durch Anklicken des Links auf eine Seite des Paketdienstleisters und kann dort sehen, wann seine Sendung ankommt.

# 7.9 Auskunftspfiichten von Online-Händlern

Beim Online-Shopping geht die Ware an den Kunden, der Händler bekommt dafür das geforderte Geld. Zugleich erhält er ein weiteres wertvolles Gut: die Daten des Kunden. Der Käufer kann vom Händler Auskunft darüber verlangen, welche Daten dieser über ihn hat. Das war bereits unter dem alten Bundesdatenschutzgesetz so und ist nun in erweiterter Form in der inzwischen geltenden Datenschutz-Grundverordnung geregelt.

Welche Daten hat eigentlich mein Online-Händler über mich? Das fragte sich der Kunde eines Internetunternehmens und bat dieses um Auskunft.

Von dort erhielt er jedoch keine Antwort, weshalb er sich hilfesuchend an mich als zuständige Datenschutzaufsichtsbehörde wandte. Zu Recht, denn die nicht (bzw. nicht richtig oder nicht rechtzeitig) erteilte Auskunft über die gespeicherten personenbezogenen Daten stellt einen Verstoß dar, der von mir geahndet werden kann.

Auskunftsanspruch schon im alten Recht

Der Vorfall ereignete sich kurz vor Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO). Deshalb ersuchte ich das Unternehmen, dem Kunden Auskunft auf Basis der damals geltenden Rechtsgrundlage zu erteilen (§ 34 des alten Bundesdatenschutzgesetzes). Hiernach hatte der Betroffene das Recht, von der verantwortlichen Stelle (hier also vom Online-Händler) unentgeltlich Auskunft über die zu seiner Person gespeicherten Daten zu erhalten. Das Auskunftsrecht erstreckte sich auch auf Angaben zur Herkunft dieser Daten. Zudem war der Zweck der Speicherung mitzuteilen sowie die Empfänger oder Kategorien von Empfängern, an welche die personenbezogenen Daten des Betroffenen weitergegeben wurden.

Nach meiner Intervention kam das Unternehmen umgehend seiner Auskunftspflicht gegenüber dem Betroffenen nach.

## Pfiichten nach DS-GVO

Seit dem 25. Mai 2018 wird eine Auskunft auf Grundlage des Art. 15 DS-GVO erteilt. Ziel des Verordnungsgebers ist es, dass sich die betroffenen Personen der Verarbeitung ihrer Daten bewusst werden und deren Rechtmäßigkeit überprüfen können. Die Auskunftsrechte ergänzen damit die Informationspflichten, die der Verantwortliche gem. Art. 13 und Art. 14 DS-GVO zu erfüllen hat.

Ergänzung zu den Informationspflichten

Für eine Auskunft gehen die von der Datenverarbeitung betroffenen Personen wie bisher aktiv auf das verantwortliche Unternehmen zu. Eine Auskunft kann mündlich, schriftlich oder elektronisch erbeten werden.

## Überprüfung der Identität nötig

Zugleich hat das Unternehmen die Aufgabe, die Identität desjenigen zu prüfen, der um Auskunft bittet. So soll vermieden werden, dass einem unberechtigten Dritten unzulässig personenbezogene Daten übermittelt werden. Zu

diesem Zweck können der vollständige Name, die Anschrift und ggf. das Geburtsdatum abgefragt werden. Auch kann um die Übersendung einer Kopie des Personalausweises gebeten werden. In diesem Fall sollte die um Auskunft ersuchende Person die nicht erforderlichen persönlichen Daten auf der Kopie schwärzen (wie Augenfarbe, Größe, ID-Nummer, Unterschrift).

Ausweiskopie schwärzen

Ein Auskunftsersuchen muss weder eine Begründung enthalten, noch bestimmten Formvorgaben entsprechen.

## Auskunft in zwei Stufen

Die Auskunft wird abgestuft gegeben: Im ersten Schritt erhält die betroffene Person vom Verantwortlichen eine Bestätigung darüber, ob dieser überhaupt sie betreffende personenbezogene Daten verarbeitet. Falls nein, ist eine Negativauskunft zu erteilen.
Andernfalls erhält der Betroffene eine Auskunft gem. Art. 15 Abs. 1 DS-GVO, also darüber, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde). Darüber hinaus sind folgende Informationen mitzuteilen:

Inhalt der Auskunft

- Zweck der Verarbeitung
- Kategorien der verarbeiteten personenbezogenen Daten
- Empfänger bzw. Kategorien von Empfängern der Daten (die diese Daten bereits erhalten haben oder künftig noch erhalten werden)
- geplante Speicherdauer (falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer)
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden
- Hinweise auf folgende Rechte:
  - Berichtigung
  - Löschung
  - Einschränkung der Verarbeitung
  - Widerspruchsrecht gegen die Verarbeitung
  - Beschwerderecht bei einer Aufsichtsbehörde

Profiling

Sofern im Rahmen der Datenverarbeitung eine automatisierte Entscheidungsfindung einschließlich Profiling erfolgt, muss der Betroffene eine aussagekräftige Information über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen erhalten.

## Kostenlos, präzise und verständlich

Die Auskunft ist kostenfrei, auch die nach Art. 15 Abs. 3 DS-GVO auf gesonderten Antrag zur Verfügung gestellten Kopien. Das Unternehmen hat somit auch die Portokosten zu tragen. Für weitere Kopien kann allerdings ein angemessenes Entgelt gefordert werden.

Der Betroffene muss die Auskunft in präziser, transparenter, verständlicher und leicht zugänglicher Form erhalten, in einer klaren und einfachen Sprache, mündlich, schriftlich oder elektronisch. Die Informationen werden unverzüglich, in jedem Fall aber innerhalb eines Monats nach Antragseingang zur Verfügung gestellt. Diese Frist kann verlängert werden, wenn dies wegen der Komplexität und der Anzahl von Anträgen erforderlich ist. Sofern dies der Fall ist, muss das verantwortliche Unternehmen die betroffene Person innerhalb eines Monats nach Eingang des Antrags darüber mit Begründung unterrichten.

Frist: ein Monat

## 7.10 Datenweitergabe von Makler zu Makler

Eine Versicherungsmaklerin beschloss, ihre Selbständigkeit aufzugeben und zukünftig im Team eines größeren Versicherungsdienstleisters mitzuarbeiten. Ihre Kunden nahm sie mit, diese wurden von ihr darüber lediglich informiert. Ein Kunde sah durch dieses Vorgehen seine Persönlichkeitsrechte verletzt und fürchtete, dass seine personenbezogenen Daten ohne Einwilligung an Dritte weitergegeben worden seien.

Die Versicherungsmaklerin war nach ihrem Wechsel nicht mehr als eigenständige Kauffrau tätig, sondern Teil des größeren Maklerbüros. Sie brachte einen wertvollen Vermögenswert mit: die Kundendatenbank. Die darin enthaltenen Daten durch Verkauf Bestandteil der Datenbank ihres neuen Arbeitgebers werden.

Rechtsgrundlage für Übermittlung nötig

Das Vorgehen der Versicherungsmaklerin sorgt für eine Übermittlung der personenbezogenen Daten ihrer Kunden an Dritte und benötigt somit eine Rechtsgrundlage. Hierfür kommen grundsätzlich eine Einwilligung oder ein überwiegendes berechtigtes Interesse der Maklerin in Betracht.

## Abwägung von Interessen notwendig

Interessen der Maklerin vs. Interessen der Kunden

Eine Einwilligung wurde nicht eingeholt. Daher bleibt zu prüfen, inwieweit die Übermittlung der personenbezogenen Daten im Kundenstamm zur Wahrung der berechtigten Interessen der Maklerin erforderlich gewesen sein könnte. Außerdem durften dem keine überwiegenden Interessen oder Grundrechte und Grundfreiheiten der betroffenen Kunden entgegenstehen.

Es besteht ein Interesse der Maklerin, im Rahmen ihres Wechsels den Wert ihres bisherigen Unternehmens an das größere Maklerbüro zu verkaufen. Dieser Wert bildet sich maßgeblich in der Kundendatenbank ab. Es existiert kein explizites gesetzliches Verbot gegen dieses Vorgehen.

## Vernünftige Erwartungen maßgeblich

Bei der Frage, ob nicht die Interessen bzw. Grundrechte und -freiheiten der Betroffenen überwiegen, sind deren vernünftige Erwartungen maßgeblich. Es ist also entscheidend, ob die betroffenen Personen zum Zeitpunkt der Datenerhebung vernünftigerweise absehen können, dass eine Datenverarbeitung für einen bestimmten Zweck stattfinden wird.

Interessen der Kunden überwiegen

Der Kunde hatte sich seinerzeit die einzelne Versicherungsmaklerin ausgesucht. Somit ist nicht davon auszugehen, dass er die Daten, die er der Maklerin anvertraut hat, einem anderen, für ihn unbekannten Makler zur Verfügung stellen will. Gerade bei einem Vertrag mit einem Versicherungsmakler ist oft von einem besonderen Vertrauensverhältnis auszugehen. Vor diesem Hintergrund überwiegen die Interessen des betroffenen Kunden gegenüber denen der Maklerin.

Folglich konnte ich keine wirksame Rechtsgrundlage für die Übermittlung der Kundendaten an das größere Maklerbüro feststellen.

## Widerspruchslösung der bessere Weg

Betroffene aufklären und entscheiden lassen

Bei Anwendung der sog. Widerspruchslösung hätte sich die Interessenabwägung anders dargestellt. Die Maklerin hätte ihren Kunden mit einem Schreiben einen Hinweis auf den beabsichtigten Verkauf und die Übermittlung ihrer Daten an ein anderes Unternehmen geben und ihnen gleichzeitig ein Widerspruchsrecht einräumen können. Diese Umstände hätten dann in die Interessenabwägung zu ihren Gunsten eingebracht werden können. Denn betroffene Personen behalten so die Möglichkeit, selbst zu bestimmen. Sie werden über die näheren Umstände aufgeklärt und können auf dieser Basis entscheiden, ob sie sich gegen die Veräußerung ihrer Daten aussprechen möchten. Dieses Vorgehen ist grundsätzlich geeignet, die Interessen in einen angemessenen Ausgleich zu bringen

Die Versendung solcher Schreiben sollte nachweisbar sein, z. B. mithilfe von Einschreiben. Der Widerspruch muss für die betroffenen Personen zudem kostenlos sein, z. B. durch Beilegung eines frankierten Rückumschlags. Auch muss ihnen eine angemessene Frist eingeräumt werden, welche auch eine urlaubsbedingte Abwesenheit berücksichtigt und daher nicht unter zwei Wochen nach Erhalt des Schreibens liegen sollte.

Zudem hätten die Betroffenen darauf hingewiesen werden sollen, dass sie nicht verpflichtet sind, mit dem größeren Maklerbüro eine vertragliche Beziehung einzugehen, sondern den Versicherungsvertrag gegebenenfalls auch direkt mit dem Versicherer fortführen können.

# F.8. Beschäftigtendatenschutz

## 8.1 Nationale Regelung zum Beschäftigtendatenschutz möglich

Bereits in meinem Tätigkeitsbericht für 2013 und 2014 hatte ich beschrieben, dass ein bundesweites Gesetz zum Beschäftigtendatenschutz weiterhin auf sich warten lässt. Zwar ist mittlerweile die Datenschutz-Grundverordnung (DS-GVO) wirksam geworden. Dennoch ist immer noch Raum für eine nationale Regelung.

Generalklausel im alten Recht

Bis zum 24. Mai 2018 galt auch im Beschäftigtendatenschutz das Bundesdatenschutzgesetz (BDSG) in seiner alten Fassung. Konkret war er in § 32 BDSG-alt geregelt, der eine sogenannte Generalklausel enthielt: Die Daten von Beschäftigten durften grundsätzlich nur dann verarbeitet werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich war. Ein umfassendes Gesetz, in dem der Gesetzgeber Grundsatzentscheidungen für besonders sensible Einzelfragen trifft (wie die Grenzen zulässiger Kontrollen von Beschäftigten im digitalen Zeitalter), war nicht in Sicht.

### Keine Spezialregelung in DS-GVO

Die seit dem 25. Mai 2018 wirksame DS-GVO enthält keine Spezialregelung für den Beschäftigtendatenschutz. Die Zulässigkeit der Verarbeitung von Beschäftigtendaten richtet sich daher vom Grundsatz her – innerhalb der DS-GVO – nach denselben Regelungen, die auch für z.B. Kundendaten gelten. Allerdings enthält die DS-GVO im Bereich des Beschäftigtendatenschutzes (Art 88 Abs. 1 DS-GVO) eine sogenannte Öffnungsklausel. Der Rahmen, der dabei einzuhalten ist, ergibt sich aus Art. 88 Abs. 2 DS-GVO.

Mit der DS-GVO haben sich die Mitgliedstaaten der EU grundsätzlich für einen europaweit einheitlichen Datenschutz entschieden. Das bedeutet natürlich zugleich, dass sie weitgehend auf nationale „Alleingänge“ verzichten. Allerdings sieht die DS-GVO für vereinzelte Themen sogenannte Öffnungsklauseln vor. Diese erlauben zu Spezialthemen nach wie vor nationale Regelungen. Der Rahmen dafür wird durch die jeweilige Öffnungsklausel selbst in der DS-GVO vorgegeben, um zumindest einen einheitlichen Grundstandard zu gewährleisten.

Nationales Schutzniveau kann erhalten bleiben

Hatte ein EU-Mitglied vor der DS-GVO im Bereich des Beschäftigtendatenschutzes ein höheres nationales Schutzniveau, kann es dieses mithilfe der Öffnungsklausel aufrechterhalten. Zugleich wird ermöglicht, dass eine nationale Regelung nahtlos an die bisherige Regelung anknüpft. Damit werden zugleich die Auslegung unter der neuen Rechtslage und die Verwendung der bisherigen – nationalen - Rechtsprechung erleichtert.

## Deutschland knüpft an bisherige Rechtslage an

Datenverarbeitung nur für Durchführung des Arbeitsverhältnisses

Der deutsche Gesetzgeber hat von der Öffnungsklausel im Bereich des Beschäftigtendatenschutzes durch Erlass des § 26 BDSG Gebrauch gemacht (in der ab 25. Mai 2018 geltenden Fassung). Der neue Paragraph entspricht weitgehend der früheren Regelung des § 32 BDSG-alt. Weiterhin dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn dies für die Durchführung (gleichgestellt ist die Begründung bzw. Beendigung) des Beschäftigungsverhältnisses erforderlich ist. Auf diese Weise knüpft der Bundesgesetzgeber an die bisherige Rechtslage an.

Zu begrüßen ist außerdem, dass nun geregelt ist, wann im Beschäftigtenverhältnis – abgesehen von der Erforderlichkeit für die seiner Durchführung – ausnahmsweise auch eine Einwilligung in Betracht kommt. Eine autonome, freiwillige Einwilligung wäre im Über-/Unterordnungsverhältnis zwischen Arbeitgeber und -nehmer nämlich in aller Regel unwirksam. § 26 Abs. 2 BDSG gibt nun vor: Eine Einwilligung im Beschäftigungsverhältnis hat nur dann Bestand, wenn für die Beschäftigten ein rechtlicher bzw. wirtschaftlicher Vorteil erreicht wird. Ausreichend ist ebenso, wenn Arbeitgeber und Beschäftigte gleichgelagerte Interessen verfolgen.

Einwilligung für Zusatzleistung möglich

Die Einwilligung kommt von vornherein nur in solchen Punkten in Betracht, die nicht die Erbringung der Arbeitsleistung betreffen. Sie kann bei Zusatzleistungen des Arbeitgebers eine hinreichende Rechtsgrundlage sein. Dafür kommt besonders die Gestattung der Nutzung dienstlicher Infrastruktur in Betracht, wie z.B. die private Nutzung von dienstlichen Fahrzeugen bzw. von EDV des Arbeitgebers.

Auch wenn ein umfassendes Beschäftigtendatenschutzgesetz weiterhin nicht in Sicht ist: Dass der Bundesgesetzgeber von der Öffnungsklausel des Art. 88 DS-GVO Gebrauch gemacht hat, ist zu begrüßen. Zumindest konnte auf diese Weise das bisherige Niveau im Beschäftigtendatenschutz gehalten werden.

# 8.2 GPS-Überwachung von Firmenfahrzeugen

Mich erreichen immer wieder Beschwerden von Beschäftigten, dass ihre Firmenfahrzeuge von den Arbeitgebern geortet werden können. Die Ortungsdaten werden zum Teil genutzt, um die Beschäftigten zu kontrollieren, wogegen ich mehrfach vorgegangen bin.

Geräte zur Positionsbestimmung sind immer häufiger ab Werk in Fahrzeugen eingebaut. Alternativ lassen sie sich mit geringem Aufwand nachrüsten. Zum Teil können die Geräte nicht nur die Position, sondern weitergehende Informationen erheben; beispielsweise zur gefahrenen Geschwindigkeit oder zum Brems- und Beschleunigungsverhalten.

Gründe für GPS häufig nicht nachvollziehbar

Ich habe festgestellt, dass solche Geräte bei Firmenfahrzeugen immer häufiger von den Arbeitgebern auf unterschiedlichste Weise genutzt werden. Die angeführten Gründe für die zwingende Notwendigkeit der damit verbundenen Datenverarbeitung sind datenschutzrechtlich in vielen Fällen allerdings nicht nachvollziehbar.

Zunächst meinen viele Arbeitgeber, dass es sich bei den Positionsdaten der Fahrzeuge nicht um personenbezogene Daten handelt. Schließlich seien es Daten des Fahrzeuges. Sie verkennen dabei, dass sie selbst in der Lage sind, ein Fahrzeug einer bestimmten Person zuzuordnen, beispielsweise anhand von Einsatzplänen. Damit sind diese Daten also sehr wohl personenbezogen.

## Wann ist die Positionsbestimmung zulässig?

Die Antwort, wann dieses Vorgehen zulässig ist, richtet sich seit dem 25. Mai 2018 nach § 26 Abs. 1 Satz 1 des Bundesdatenschutzgesetzes (BDSG). Danach dürfen personenbezogene Daten von Beschäftigten unter anderem dann verarbeitet werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Der Arbeitgeber muss sich allerdings mit der Frage befassen, ob seine Interessen auch ohne oder mit weniger personenbezogenen Daten seiner Beschäftigten erreicht werden können. Selbst wenn dies nicht der Fall sein sollte, muss geklärt werden, ob die Verarbeitung der Beschäftigtendaten verhältnismäßig ist. Das ist nicht der Fall, wenn die Interessen der Beschäftigten überwiegen, dass ihre Daten nicht wie beabsichtigt verarbeitet werden.

Verarbeitung muss verhältnismäßig sein

Beispiele aus der Praxis sollen dies verdeutlichen:

Kosten für Spezialfahrzeuge

- In einem Fall war ein besonders aufwendig ausgestattetes Spezialfahrzeug mit einem Ortungsgerät versehen. Der Einsatz dieses Fahrzeuges sollte gegenüber den Kunden in möglichst kleinen und genauen Einheiten abgerechnet werden, wofür die Daten gespeichert, monatlich

ausgewertet und anschließend gelöscht wurden. Der Arbeitgeber hat sich zugleich selbst verpflichtet, die Daten nicht zur Verhaltens- und Leistungskontrolle zu verwenden.

- Zulässig kann die Erhebung der jeweils aktuellen Position – ohne längerfristige Speicherung – auch sein, wenn die Standorte zur Live-Disposition notwendig sind und sich der Arbeitgeber verpflichtet, die Daten nicht zur Verhaltens- und Leistungskontrolle zu verwenden. Denkbar ist dies besonders bei Speditionen, damit die Leitzentrale etwa Staus frühzeitig erkennen und darauf reagieren kann. Beispielsweise wenn der Empfänger über spätere Lieferungen informiert werden muss (z.B. bei Just-in-time-Belieferung).

Live-Disposition

- Denkbar ist auch, dass Daten zum Nachweis erbrachter Arbeitsleistungen etwas länger gespeichert werden, wenn andernfalls mit hohen wirtschaftlichen Schäden zu rechnen ist. Hier kommen vor allem Winterdienstleistungen in Betracht. Werden diese nur unzureichend erbracht, kann das mit erheblichen körperlichen Folgen für Unfallopfer sowie mit wirtschaftlichen Folgen für den Dienstleister verbunden sein. Auch hier ist wichtig, dass der Arbeitgeber die Daten nicht für Leistungs- und Verhaltenskontrollen verwendet. Zudem könnte geregelt werden, dass der Zugriff auf die gespeicherten Daten nur im Vier-Augen-Prinzip oder mittels aufgeteilter Passwörter möglich ist. Zu Beginn der jeweils folgenden Winterdienstsaison sollten die Daten dann gelöscht werden.

Winterdienst

## Wann ist die Positionsbestimmung nicht zulässig?

Wenn der Verantwortliche die Daten nur deshalb speichert, um ggf. einem Vertragspartner nachweisen zu können, dass er eine Leistung erbracht hat, ist dies in der Regel nicht zulässig.

So habe ich in einem Fall die Nutzung der Positionsbestimmung stark eingeschränkt. Bei den betroffenen Beschäftigten handelte es sich um Objektbetreuer im Reinigungsgewerbe. Diese Kräfte fahren jeden Standort mehr oder weniger regelmäßig an. Sie planen ihre Arbeitstage und Fahrstrecken selbstständig und dürfen die Fahrzeuge im Rahmen der steuerlichen 1-Prozent-Regelung privat nutzen. Der Arbeitgeber speicherte die genauen Fahrzeiten und Standorte seiner Mitarbeiter über ein knappes halbes Jahr – auch außerhalb der Arbeitszeit. Mit Blick darauf, dass die Beschäftigten ihre Arbeitstage selbst planen und sie in ihrer Freizeit keine Überwachung durch den Arbeitgeber dulden müssen, habe ich die Erhebung und Speicherung sowohl während als auch außerhalb der Arbeitszeit beschränkt. Das Unternehmen darf Positionsdaten nur noch verarbeiten, wenn das Fahrzeug als gestohlen gemeldet wird.

Keine Erhebung außerhalb der Arbeitszeit

Ein Argument der Arbeitgeber ist häufig, dass die Daten für die Planung von Touren genutzt werden. Diese Argumentation läuft jedoch ins Leere. Solche Pläne werden regelmäßig mithilfe einer speziellen Software oder eines Webdienstes gemacht, welche Prognosen für die Verkehrsdichte erstellen und automatisch einbeziehen. Bislang konnte mir kein Unternehmen plausibel darlegen, warum ein Rückgriff auf vergangene Daten notwendig ist, um künftige Routen zu planen.

Auch das Argument, dass die Daten für ein Fahrtenbuch benötigt werden, greift nicht. Von der Finanzverwaltung und von den Straßenverkehrsbehörden werden Fahrtenbücher akzeptiert, die einen überschaubaren Datensatz an Informationen enthalten. Die mit GPS-Systemen erfassten Informationen gehen gewöhnlich deutlich darüber hinaus. Werden durch ein GPS-gestütztes

GPS für Fahrtenbuch nicht nötig

Fahrtenbuch hingegen nur die Informationen verarbeitet, die für ein Fahrtenbuch tatsächlich notwendig sind, wäre das nicht zu beanstanden. Das sind in der Regel: Datum, Start- und Endpunkt, gefahrene Kilometer, Kilometerstand, Fahrtzweck.

## Hohe Anforderungen an heimliche Überwachung

Zunehmend erreichen mich Eingaben, in denen sich Beschäftigte wegen heimlicher Überwachung ihrer Aufenthaltsorte beschweren. Offenbar verwenden Arbeitgeber die in Fahrzeugen und Navigationsgeräten integrierten Funktionen nun auch häufiger ohne Wissen der Beschäftigten und zur Verhaltens- und Leistungskontrolle.

Straftaten aufdecken

Die heimliche Überwachung von Beschäftigten ist jedoch mit hohen Anforderungen verbunden. Typischerweise ist dies nur zulässig, wenn tatsächliche, zu dokumentierende Anhaltspunkte dafür vorliegen, dass der Überwachte im Beschäftigungsverhältnis eine Straftat begangen hat. Außerdem muss die heimliche Überwachung geeignet sein, die Straftat aufzudecken (§ 26 Abs. 1 Satz 2 BDSG).

Informationspflichten beachten

Vor einer heimlichen Überwachung der Beschäftigten ist in allen anderen Konstellationen zu warnen. Zunächst müssen Arbeitgeber grundsätzlich ihrer Informationspflicht aus Art. 13, 14 DS-GVO gegenüber den Beschäftigten nachkommen. Die Arbeitgeber müssen also darüber informieren, dass Positionsdaten der Beschäftigten erhoben werden und zu welchem Zweck dies erfolgt. Unterlassen Arbeitgeber diese Information, drohen Bußgelder bis zu 20 Millionen Euro oder – falls dieser Wert höher sein sollte – 4 Prozent des Weltjahresumsatzes. Das gilt selbst dann, wenn die eigentliche Verarbeitung zulässig sein sollte.

# 8.3 Mistery Calls zur Leistungskontrolle

Mit so genannten Mystery Calls wollen Arbeitgeber die Qualität der Beratung durch ihre Beschäftigten überprüfen. Dazu rufen gewöhnlich externe Dritte bei den Beschäftigten an und lassen sich von ihnen beraten. Dies geschieht zum Teil ohne Wissen der Beschäftigten.

Bedarf für Fortbildungen feststellen

Bei systematischen Mystery Calls handelt es sich um eine Art der Leistungskontrolle durch den Arbeitgeber. Sie dienen häufig dem Zweck, Fortbildungsbedarfe bei den Beschäftigten zu identifizieren. Der Mystery Call ist daher Teil der Qualitätssicherung. Der Fortbildungsbedarf kann fachlicher Natur sein, sodass ggf. inhaltliche (Nach-)Schulungen nötig sind. Außerdem kann ein persönlich-individueller Fortbildungsbedarf identifiziert werden, wenn beim telefonischen Umgang Verbesserungspotenzial erkannt wird.

Beschwerden von Kunden überprüfen

Werden Mystery Calls lediglich punktuell eingesetzt, ist das Ziel des Arbeitgebers keine allgemeine Qualitätssicherung. Grund solcher Maßnahmen können Beschwerden von Kundinnen und Kunden sein, welche nachvollzogen werden sollen. Alternativ könnte der Mystery Call von einem Arbeitgeber eingesetzt werden, um Argumente für eine verhaltens- oder leistungsbasierte Kündigung zu sammeln.

Die Zulässigkeit solcher Anrufe ist seit dem 25. Mai 2018 nach § 26 Bundesdatenschutzgesetz (BDSG) zu beurteilen. Danach dürfen personenbezogene Daten von Beschäftigten unter anderem dann verarbeitet werden, wenn es zur Durchführung des Beschäftigungsverhältnisses erforderlich ist.

## Eignung abhängig vom Arbeitsplatz

Ob Mystery Calls überhaupt ein geeignetes Mittel für die Qualitätssicherung darstellen, muss man anhand des Arbeitsplatzes beurteilen. Wenn Telefonate mit Kundinnen und Kunden nur einen untergeordneten Teil der Arbeitsleistung ausmacht, sind Mystery Calls eher ungeeignet. Die Leistung der Beschäftigten kann dann typischerweise auf anderem Wege beurteilt werden; beispielsweise anhand ihrer erarbeiteten Unterlagen. Laufen Beschwerden über Beschäftigte auf, können diese außerdem zunächst ohne solche Maßnahmen thematisiert werden.

Mithören in begrenztem Umfang zulässig

Machen Telefonate mit Kundinnen und Kunden hingegen einen erheblichen Anteil der individuellen Arbeitsleistung aus, stehen dem Arbeitgeber nur wenige Möglichkeiten zur Verfügung, die Leistung seiner Beschäftigten einzuschätzen. Für den Call-Center-Bereich lässt sich festhalten, dass in überschaubarem Umfang ein Mithören von Gesprächen mit dem Ziel der Qualitätssicherung zulässig ist.

Ist die Arbeitsleistung – ähnlich einem Call Center – von telefonischen Kundenberatungen geprägt, könnte als Alternative zum Mithören auch ein Mystery Call in Betracht kommen. Während das Mithören im Call Center durchaus offen stattfinden kann (und sollte), ist ein Mystery Call stets auf Heimlichkeit angelegt. Die Beschäftigten sollen gerade nicht mitbekommen, dass sie vom Arbeitgeber bewertet werden.

Ständiger Überwachungsdruck

Könnte ein heimlicher Mystery Call jederzeit erfolgen, würde damit ein ständiger Überwachungsdruck erzeugt. Die Maßnahme wäre in diesem Fall datenschutzrechtlich unzulässig. Zwar könnte sich eine Kundin oder ein Kunde jederzeit beschweren. Eine solche Beschwerde setzt sich jedoch nicht mit zahlreichen Aspekten des Telefonats auseinander, sondern beschränkt sich auf einige wenige Punkte. Die Leistungskontrolle über Mystery Calls stellt im Vergleich einen deutlich stärkeren Eingriff dar.

## Gezielt und transparent durchführen

Umfassende Informationen im Vorfeld

Der Überwachungsdruck kann vermieden werden, indem Mystery Calls verhältnismäßig selten durchgeführt und die Beschäftigten vorab informiert werden. Die Information muss einen konkreten und möglichst kurzen Zeitraum – höchstens wenige Tage – benennen, an denen es zu solchen Anrufen kommen kann. Insgesamt sollten Mystery Calls nur an wenigen Tagen im Jahr überhaupt in Betracht kommen. Weiterhin sollte der Arbeitgeber offenlegen, was konkret bewertet werden soll.

Wird ein externer Dienstleister für die Durchführung von Mystery Calls eingesetzt, kann dies zur Objektivierung der Ergebnisse beitragen. Auch kann auf diesem Weg möglicherweise eine höhere Akzeptanz auf Seiten der Beschäftigten erreicht werden.

Gespräche nicht aufzeichnen

Eine Speicherung des geführten Gesprächs kann regelmäßig nicht auf § 26 BDSG gestützt werden. Es bedürfte vielmehr einer besonderen Rechtsvorschrift, die solch eine Aufzeichnung erlaubt. Vor dem Hintergrund des § 201 Strafgesetzbuch (StGB) – Verletzung der Vertraulichkeit des Wortes – ist auch unter strafrechtlichen Gesichtspunkten dringend von Aufzeichnungen abzuraten.

## Ergebnisse nicht zu breit streuen

In einem Fall habe ich feststellen müssen, dass die Ergebnisse einer Mystery Call-Runde innerhalb des Unternehmens nicht hinreichend vertraulich behandelt wurden. Die vollständige Auswertung – für alle Beschäftigten, teilweise mit Freitextfeldern – wurde nicht nur den jeweiligen Vorgesetzten zur Kenntnis gegeben, sondern sämtlichen Abteilungsleitungen. In einem Gespräch mit meiner Behörde hat der Arbeitgeber zugesichert, die Verbreitung künftig auf den jeweils erforderlichen Personenkreis zu beschränken.

# 8.4 Wer pfiegt meine Angehörigen?
## Familien wünschen Auskünfte

Mich haben mehrere Anfragen von Angehörigen zu Dokumentationen bei Pflegediensten und Pflegeheimen erreicht. Die Angehörigen interessierte, welche Beschäftigten ihre Angehörigen konkret gepflegt hatten Die Dienste bzw. Heime haben dies jeweils unter Hinweis auf den Datenschutz abgelehnt.

Gewöhnlich wollten die Angehörigen, dass ich Verstöße gegen datenschutzrechtliche Vorschriften feststelle. Sie wollten über mich erreichen, dass die Dienste bzw. Heime ihnen die Daten mitteilen. Abgesehen von speziellen datenschutzrechtlichen Auskunftspflichten ist es allerdings nicht meine Aufgabe, gegenüber Verantwortliche solche Auskünfte anzuordnen.

Zivilrechtliche Ansprüche

Auskunftsansprüche könnten sich allerdings auf den zivilrechtlichen Vertrag stützen, der mit den Pflegediensten bzw. -heimen abgeschlossen wurde. Sollten sich die Verantwortlichen weigern, können Angehörige dann etwaige Ansprüche vor den ordentlichen Gerichten durchsetzen.

### Keine Grundlage im Bundesdatenschutzgesetz

Personenbezogene Daten von Beschäftigten dürfen grundsätzlich nur verarbeitet werden, wenn dies nach § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Dass eine Weitergabe an Angehörige für die Durchführung des Beschäftigungsverhältnisses erforderlich sein könnte, liegt nicht auf der Hand.

Interessenabwägung erforderlich

Kann die Weitergabe nicht auf das BDSG gestützt werden, kommt Art. 6 Abs. 1 lit. f der Datenschutz-Grundverordnung (DS-GVO) als Rechtsgrundlage in Betracht. Beabsichtigt der Arbeitgeber, Daten seiner Beschäftigten weiterzugeben, muss er eine Interessenabwägung durchführen. Die Verarbeitung müsste zur Wahrung der berechtigten Interessen des Arbeitgebers oder eines Dritten erforderlich sein. Hier könnte der Angehörige – als Dritter – ein solches Interesse haben.

Sicherheitsinteresse

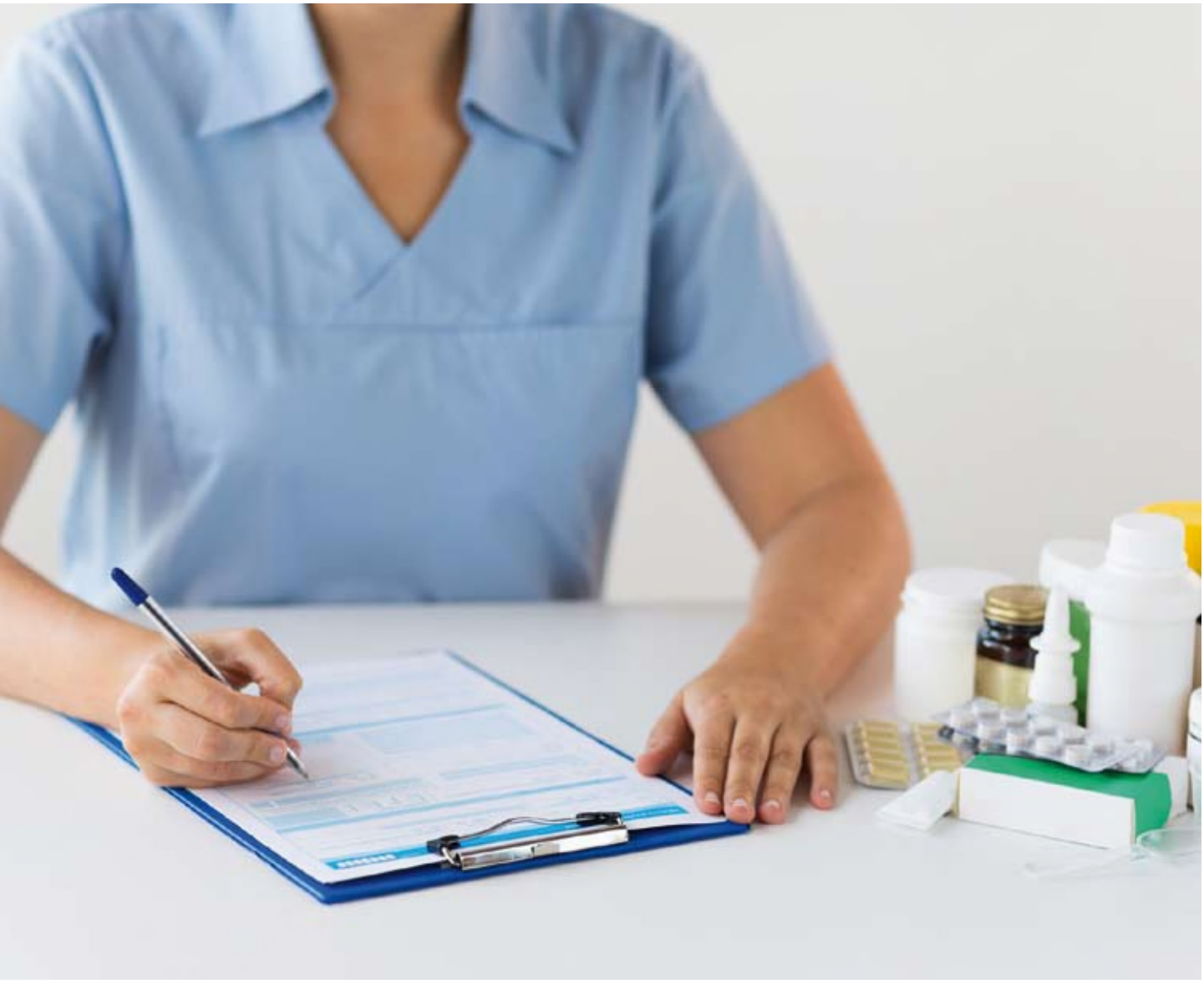
Allerdings dürfen die Interessen bzw. Grundrechte und Grundfreiheiten der betroffenen Beschäftigten nicht überwiegen. Ein Recht darauf, Arbeitsleistungen anonym zu erbringen, gibt es nicht. Steht jedoch zu befürchten, dass die Daten missbraucht werden, können die Interessen der Beschäftigten überwiegen. Das könnte der Fall sein, wenn durch Angehörige bereits Drohungen gegen Leib und Leben der Beschäftigten ausgesprochen wurden und anhand der begehrten Daten weitere Informationen über die Beschäftigten erlangt werden könnten (z.B. Privatanschrift oder private Telefonnummer).

Wer hat gefragt?

Bei der Interessenabwägung muss der Arbeitgeber weiterhin berücksichtigen, wem die Daten mitgeteilt werden sollen. Die Interessen einer Betreuerin oder eines Betreuers sind dabei höher einzuschätzen als die Interessen (anderer) Angehöriger. Im Ergebnis kann es daher zulässig sein, die Nachnamen der eingesetzten Beschäftigten an Betreuerinnen und Betreuer weiterzugeben.

Vor diesem Hintergrund ist es häufig nur vorgeschoben, Auskünfte aus „datenschutzrechtlichen Gründen“ abzulehnen. Gründe können sein, dass der Dienst bzw. das Heim sich nicht näher mit dem Datenschutzrecht befasst haben oder dass Strukturen verschleiert werden sollen (beispielsweise häufig wechselnde Hilfskräfte).

Unabhängig vom Ergebnis einer Interessenabwägung ist der Arbeitgeber nicht aufgrund des Datenschutzrechts verpflichtet, solche Auskünfte zu erteilen. Gleichwohl könnte sich ein solcher Anspruch aus dem zivilrechtlichen Vertrag ergeben.



# 8.5 Entbindung von der Schweigepfiicht bei Arbeitseinsätzen im Ausland

Hat ein Arbeitnehmer im Ausland einen Unfall, ist es für Angehörige und Arbeitgeber häufig schwierig Informationen über den Gesundheitszustand des Betroffenen zu erhalten. Notwendige Voraussetzung ist eine Erklärung zur Entbindung von der Schweigepflicht durch den Arbeitnehmer.

Im Rahmen einer Beratung im Jahr 2017 hat ein Unternehmen an mich herangetragen, dass Beschäftigte im Auslandseinsatz gelegentlich Unfälle haben und anschließend nicht immer ansprechbar sind. Künftig möchte das Unternehmen zuverlässig Informationen zum allgemeinen Gesundheitszustand erhalten und diese an die Angehörigen weitergeben können. Dazu war beabsichtigt, von den Beschäftigten Erklärungen zur Entbindung von der Schweigepflicht einzuholen.

Das Muster der Erklärung wurde mir im Rahmen der Beratung vorgelegt. Damit sollten die behandelnden Ärzte Auskunft gegenüber dem Betriebs- oder Hausarzt des Betroffenen erteilen können. Das Unternehmen zog in Betracht, die Erklärungen zentral zu verwalten und bei Bedarf zu verwenden.

Zentrale Verwaltung geplant

## Erklärung muss freiwillig sein

Beschäftigte können zu einer solchen Erklärung nicht verpflichtet werden. Bei der Erklärung zur Entbindung von der Schweigepflicht handelt es sich um eine Einwilligung im datenschutzrechtlichen Sinn. Diese muss freiwillig abgegeben werden, um wirksam zu sein.

Zwar ist es zulässig, den Beschäftigten ein Formular zur Verfügung zu stellen, das diese ausfüllen können. Die Formulare zwingend beim Unternehmen zu hinterlegen, ging aus meiner Sicht aber zu weit. Schon indem das Unternehmen kontrolliert, ob die ausgefüllten Formulare vorgelegt werden, könnte Druck auf die Beschäftigten ausgeübt werden, die Erklärung abzugeben. Es ist nicht notwendig, dass der Arbeitgeber erhebt, welche Beschäftigten eine freiwillige Erklärung abgegeben haben bzw. an welche Ärzte etwaige Befunde weitergegeben werden sollen.

Kontrolle des Rücklaufs erzeugt Druck

## Empfehlungen für Ergänzungen

Da im Vorfeld unklar ist, wer bei eine, Unfall der behandelnde Arzt sein wird, kann die Erklärung kaum konkretisiert werden. Um das Missbrauchspotenzial zu reduzieren, habe ich Ergänzungen bzw. Einschränkungen empfohlen. So

Potenzial zum Missbrauch reduzieren

sollte die Erklärung nur dann wirksam sein, wenn der Patient den eigenen freien Willen nicht äußern kann. Kann der freie Wille geäußert werden, kann der Patient eine entsprechende Erklärung selbst abgeben. Darüber hinaus kann die Erklärung auf die Zeiträume des Auslandsaufenthalts befristet werden.

## Original-Erklärung vor Ort aufbewahren

Die angedachte zentrale Verwaltung beim Arbeitgeber erschien mir nicht geeignet. Solche Erklärungen werden häufig im Original benötigt. Wenn sie zentral verwaltet werden, müssten sie zunächst von der Zentrale ins Ausland gebracht werden. Es erschien mir deshalb sinnvoller, die Erklärungen im Original in verschlossenen Umschlägen an den jeweiligen Arbeitsplätzen im Ausland abzulegen. Die Umschläge könnten entsprechend gekennzeichnet werden und im Bedarfsfall von Kollegen an den behandelnden Arzt weitergegeben werden.

Zusätzliche Erklärung nötig

Ich habe darüber hinaus grundlegende Zweifel geäußert, dass die Erklärung zur Entbindung von der Schweigepflicht den geplanten Zweck überhaupt erfüllen kann. Zwar würden damit behandelnde Ärzte ermächtigt, den Betriebs- oder Hausarzt zu unterrichten. Diese wiederum sind allerdings ohne zusätzliche Entbindungserklärung nicht befugt, dem Arbeitgeber oder den Angehörigen Auskünfte zu erteilen.

Denkbare Alternative: Notfallkarte

Zweckmäßiger erschien mir eine mehrsprachige „Notfallkarte“, welche von den Beschäftigten handschriftlich ausgefüllt werden kann. Ähnlich einem Organspenderausweis könnten ein oder zwei Kontaktpersonen angegeben werden. Eine entsprechende Formulierung vorausgesetzt, könnten die Kontakte im Notfall benachrichtigt und ggf. allgemein über den Zustand des Patienten informiert werden. Der Beschäftigte könnte frei entscheiden, ob er auf der Karte Familienangehörige, behandelnde Ärzte und/oder andere Beschäftigte als Kontakte angibt.

## Praktikable und datenschutzgerechte Lösung

Fürsorgepflicht des Arbeitgebers

Hintergrund der Anfrage war für das Unternehmen die Fürsorgepflicht gegenüber Beschäftigten einerseits und deren Angehörigen andererseits. Für die Angehörigen stellen der Arbeitgeber bzw. die ebenfalls vor Ort eingesetzten Kollegen häufig die einzige kurzfristig verfügbare Verbindung dar, wenn Beschäftigte einen Unfall hatten.

Dem Unternehmen ging es erkennbar nicht darum, gesundheitliche Details über seine Beschäftigten in Erfahrung zu bringen. Stattdessen wollte es vermeiden, dass es selbst und Angehörige länger als nötig in Ungewissheit gehalten werden. Ich habe mich daher für eine möglichst praktikable und zugleich datenschutzgerechte Lösung eingesetzt.

# F.9. Videoüberwachung

## 9.1 Videoüberwachung in Bus und Bahn

Per Anordnung wollte ich dem Verkehrsbetrieb ÜSTRA aufgeben, die Videoüberwachung in Bussen und Stadtbahnen einzustellen. Das Oberverwaltungsgericht (OVG) Lüneburg sah die Kameras allerdings als zulässig an und ließ keine Revision gegen sein Urteil zu. Um diese wichtige Frage doch noch höchstrichterlich klären zu lassen, habe ich Nichtzulassungsbeschwerde eingelegt.

OVG: Kameras sind zulässig

Mit seinem Urteil vom 7.Septemer 2017 entschied das OVG Lüneburg, dass die in den Fahrzeugen der ÜSTRA fest installierten Videokameras datenschutzrechtlich zulässig sind[1]. Sie zeichnen durchgehend Bilder vom gesamten Fahrzeuginnenraum auf, um Beweise bei Vandalismus zu sichern oder andere Straftaten verfolgen zu können.

Das OVG urteilte, das permanente Filmen diene der Verhütung und Verfolgung von Straftaten, die im Zusammenhang mit der Fahrgastbeförderung stehen. Die ÜSTRA habe nachweisen können, dass es in der Vergangenheit zu zahlreichen sicherheitsrelevanten Vorfällen gekommen sei, die die Erforderlichkeit der Videoüberwachung begründen.

### OVG: Schutzinteressen der ÜSTRA überwiegen

Gericht sieht nur geringen Grundrechtseingriff

Anhaltspunkte für das Überwiegen schutzwürdiger Interessen der betroffenen Fahrgäste sah das Gericht nicht. Zwar greife die Kameraüberwachung in das Recht auf informationelle Selbstbestimmung und in das Recht am eigenen Bild ein. Jedoch sei dieser Grundrechtseingriff als gering anzusehen, denn das Bildmaterial werde nur für 24 Stunden gespeichert und unbesehen gelöscht, wenn es zu keinem sicherheitsrelevanten Vorfall gekommen ist.

Demgegenüber stünden zum Teil gewichtige Rechtsgüter, die mit Hilfe der Videoüberwachung geschützt werden sollen. Hierzu zählen der Schutz von Leben, Gesundheit und Freiheit der Fahrgäste sowie der Schutz des Eigentums vor Straftaten. Auch das subjektive Sicherheitsbedürfnis der Fahrgäste sei ein zu berücksichtigendes Schutzgut im Rahmen der Interessenabwägung.

1 : 11 LC 59/16 und 10 A 4379/15

## Nichtzulassungsbeschwerde wegen grundsätzlicher Bedeutung

Das OVG Lüneburg ließ keine Revision gegen seine Entscheidung zu. Allerdings betrachte ich die Frage, wie und in welchem Umfang eine Videoüberwachung im öffentlichen Personennahverkehr datenschutzrechtlich zulässig ist, von grundsätzlicher Bedeutung. Nahezu alle Verkehrsbetriebe - auch in anderen Bundesländern – statten ihre Fahrzeuge zunehmend mit Videotechnik aus, um dem öffentlichen Ruf nach mehr Sicherheit zu entsprechen. Daher habe ich mich entschieden Nichtzulassungsbeschwerde einzulegen, um dem Bundesverwaltungsgericht die Möglichkeit zu geben, diese Rechtsfrage verbindlich zu beantworten.

Massenhafte und anlasslose Speicherung

Eine ständige Videoüberwachung in allen Fahrzeugen greift in unverhältnismäßiger Weise in die Grundrechte der Fahrgäste ein. Die Bildaufnahmen werden zwar nur für 24 Stunden gespeichert und dann automatisch gelöscht, wenn kein Anlass für eine Auswertung besteht. Jedoch ähnelt diese Vorgehensweise einer Speicherung von Datenmaterial auf Vorrat. Daten aller Fahrgäste werden verarbeitet unabhängig davon, ob diese durch ihr Verhalten dazu Anlass gegeben haben. Die massenhafte und anlasslose Speicherung von Daten über Personen, die sich rechtskonform verhalten, ist aber ein schwerwiegender Grundrechtseingriff.

## Neue Voraussetzungen durch DS-GVO

Eine Entscheidung des Bundesverwaltungsgerichts ist auch deshalb von besonderem rechtlichen Interesse, weil seit Mai 2018 für die Videoüberwachung im ÖPNV die neuen Regelungen der Datenschutz-Grundverordnung (DS-GVO) gelten. Die Entscheidung des OVG Lüneburg stützt sich maßgeblich auf § 4 des Bundesdatenschutzgesetzes (BDSG) zur Videoüberwachung öffentlich zugänglicher Räume. Danach hat im Rahmen der notwendigen Interessenabwägung bei einer Videoüberwachung in Fahrzeugen der Schutz der Sicherheit der beförderten Personen besonderes Gewicht.

Rechtsfrage muss dem EuGH vorgelegt werden

Nach Lesart der Datenschutzbeauftragten der Länder[2] ist § 4 BDSG aber spätestens seit dem Wirksamwerden der DS-GVO europarechtswidrig. Denn diese trifft mit Art. 6 Abs. 1 f) DS-GVO eine abschließende Regelung zur Videoüberwachung in öffentlichen zugänglichen Räumen durch nicht-öffentliche Stellen. Insofern hätte meiner Ansicht nach schon das OVG Lüneburg diese Rechtsfrage dem EuGH zur Beantwortung vorlegen müssen.

Bei Redaktionsschluss dieses Berichts war noch nicht über die Nichtzulassungsbeschwerde entschieden.

2 Vgl. Entschließung der 92. DSK vom 09.11.2016: „Videoüberwachungsverbesserungsgesetz zurückziehen!"

# 9.2 Dashcams im Straßenverkehr

Dashcams werden bei Autofahrern immer beliebter. In der Regel sind sie aber datenschutzrechtlich unzulässig. Das wurde auch in einem Klageverfahren deutlich, das „Knöllchen-Horst" gegen meine Behörde angestrengt hatte. Inzwischen gibt es zum Dashcam-Einsatz im Straßenverkehr ein Urteil des Bundesgerichtshofes.

In früheren Berichten habe ich dargelegt, dass der Einsatz von Dashcams (auch wenn sie von Privatpersonen eingesetzt werden) an den Regelungen des Bundesdatenschutzgesetzes in alter Fassung zu messen ist[1]. Das gilt, soweit in öffentlich zugänglichen Bereichen gefilmt wird und als Hauptzweck die Weitergabe von Filmaufnahmen zur Dokumentation eines Unfallhergangs angegeben wird. Danach ist eine Beobachtung und Aufzeichnung mit Videokameras nur zulässig, wenn es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Außerdem dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen (also der anderen Verkehrsteilnehmer) überwiegen.

Interessen der anderen Verkehrsteilnehmer überwiegen

Diese Voraussetzungen sind in aller Regel beim Einsatz einer Dashcam nicht erfüllt, da die schutzwürdigen Interessen der anderen, meist unbeteiligten Verkehrsteilnehmer überwiegen. Das Recht auf Schutz der personenbezogenen Daten einer Person aus Art. 8 der Charta der Grundrechte der Europäischen Union 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.

## Vielzahl von Personen unter Generalverdacht

Dauerhaft aufzeichnende Dashcams erfassen permanent und ohne Anlass den Verkehr und Personen. So ist eine Vielzahl von Verkehrsteilnehmern betroffen, die unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung wissen oder sich ihr entziehen können. Der Autofahrer hat das Interesse, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zu haben. Dieses Interesse kann aber den gravierenden Eingriff in das Recht auf Schutz der personenbezogenen Daten der Verkehrsteilnehmer nicht rechtfertigen.

Aus diesem Grund hatte ich bereits in der Vergangenheit angekündigt: Werden wiederholt Dashcams zur Dokumentation von Straftaten, Verkehrsordnungswidrigkeiten oder eines Unfallhergangs eingesetzt, werde ich ein Bußgeldverfahren einleiten. Nötigenfalls werde ich außerdem den Dashcam-Einsatz durch Erlass einer Anordnung unterbinden.

Bußgelder bei wiederholtem Einsatz

1 § 6b Abs. 1 Nr. 3 und Abs. 3 BDSG-alt

## Eindeutiges Urteil zu „Knöllchen-Horst“

Ein in der Presse als „Knöllchen-Horst“ bekannter Mann hatte es sich zur Aufgabe gemacht, vermeintliche oder tatsächliche Verkehrsverstöße anzuzeigen, auch wenn er selbst nicht betroffen war. Als Beweismittel hatte er auf Fotos und Videos der an Front- und Heckscheibe seines Fahrzeugs befestigten Dashcams zurückgegriffen.

Kurz nachdem ich für den Fall eines erneuten Dashcam-Einsatzes sowohl das Bußgeld- als auch das Untersagungsverfahren angedroht hatte, gingen die nächsten Anzeigen beim Landkreis Osterode ein.

Verweis auf Videoüberwachung der Polizei

Die im Rahmen des aufsichtsbehördlichen Kontrollverfahrens geforderten Auskünfte wurden nicht vollständig erteilt. Stattdessen berief sich „Knöllchen-Horst“ auf die umfangreiche Videoüberwachung durch die Bahn und die Polizei, welche nicht durch die Aufsichtsbehörden beanstandet würden. Auch im Rahmen einer Anhörung verwies er auf die Videoüberwachung in anderen Fällen und auf das Recht zur Anzeigenerstattung. Zu seiner selbst durchgeführten Überwachung mit Dashcams gab es keine Aussagen. Da der Dashcam-Betreiber seiner Auskunftspflicht nicht nachkam, habe ich nach Androhung ein Zwangsgeld festgesetzt, gegen das Klage eingereicht wurde.

Noch während dieses Klageverfahren anhängig war, legte „Knöllchen-Horst“ erneut Anzeigen mit Aufnahmen seiner Dashcams vor. Daher untersagte ich mit sofortiger Wirksamkeit in einer weiteren Verfügung den Einsatz der Dashcams zum Zweck der Anzeigenerstattung.

Auch gegen diese Anordnung legte er Klage ein und beantragte einstweiligen Rechtsschutz.

VG Göttingen weist Klagen ab

Das Verwaltungsgericht Göttingen wies die Klagen im Mai 2017 ab[2]. Auf eine persönliche oder familiäre Tätigkeit könne sich der Kläger schon allein deshalb nicht berufen, da er die Dashcam-Aufnahmen im Rahmen der Anzeigenerstattung an den Landkreis übermittelt habe. Das Verwaltungsgericht stellte fest, dass eine Videoüberwachung, die sich auch nur teilweise auf den öffentlichen Raum erstrecke und dadurch auf einen Bereich außerhalb der Sphäre desjenigen gerichtet sei, der die Daten verarbeite, nicht als eine ausschließlich persönliche oder familiäre Tätigkeit angesehen werden könne. Der Datenschutz sei daher zu beachten. Zu Kfz-Kennzeichen stellte das VG Göttingen nochmals klar, dass diese – genau wie GPS-Standortdaten – personenbezogene Daten seien. Auf welche Weise der Betroffene identifiziert werden könne, sei unerheblich. Bestimmbar sei eine Person bereits dann, wenn aus dem Datum Rückschlüsse auf sie möglich sind und sie sich damit individualisieren lasse.

Verfolgung von Straftaten ist Aufgabe der Behörden

Das Gericht stellte schließlich fest, dass die Beobachtung und Aufzeichnung anderer Verkehrsteilnehmer zur Sicherung von Beweismaterial bei Verkehrsverstößen keine schützenswerten eigenen Interessen darstellen würden. Selbst wenn man ein schutzwürdiges Interesse des Klägers annähme, würden Anhaltspunkte bestehen, dass die schutzwürdigen Interessen der anderen Verkehrsteilnehmer (auch Fußgänger) mit ihrem Recht auf informationelle Selbstbestimmung die Interessen des Klägers auf Selbst- und Eigentumsschutz ohne konkrete Gefährdung überwiegen. Denn für diese bestehe die Gefahr, dass sie aufgrund der Anzeigen des Klägers zu Unrecht mit Verfahren überzogen werden. Die Aufgabe der Verfolgung von Ordnungswidrigkeiten oder Straftaten obliege aber nicht dem Kläger, sondern den hierfür zuständigen Behörden.

2 VG Göttingen, Urteil vom 31.05.2017, 1 A 170/16

## Gerichte bestätigen Bußgeld

Da der Kläger des verwaltungsgerichtlichen Verfahrens sich uneinsichtig zeigte, habe ich zusätzlich ein Ordnungswidrigkeitenverfahren geführt. Gegen das von mir festgesetzte Bußgeld legte der Kläger Einspruch ein. Es kam daher im April 2017 zur Verhandlung vor dem Amtsgericht Hannover.

Das Amtsgericht urteilte, dass die Videoaufzeichnung im öffentlichen Straßenverkehr einen Verstoß gegen Bestimmungen des Bundesdatenschutzgesetzes darstellt. Die Aufzeichnungen enthielten erkennbare Gesichter sowie ablesbare Fahrzeug-Kennzeichen, also personenbezogene Daten. Die Festsetzung des Bußgeldes wurde daher vom Amtsgericht bestätigt.

Der Betroffene war mit der Entscheidung des Amtsgerichtes nicht einverstanden. Er legte sofortige Beschwerde ein, mit der sich das Oberlandesgericht (OLG) Celle befasste. Das OLG bestätigte das Urteil des Amtsgerichtes im Ergebnis und stellte darüber hinaus fest, dass die Tat vorsätzlich begangen wurde[3].

In Zukunft höhere Bußgelder

Mit 250 Euro fiel das Bußgeld gegen „Köllchen-Horst“ noch sehr gering vor. Die Datenschutz-Grundverordnung sieht nun einen weit größeren Bußgeldrahmen vor als das bis dahin geltende Recht. Vor diesem Hintergrund werde ich in Zukunft in vergleichbaren Fällen höhere Bußgelder festsetzen.

## Entscheidung des BGH zur Dashcam

Permanente Aufzeichnungen verstoßen gegen Datenschutz

Inzwischen gibt es zum Einsatz von Dashcams im Straßenverkehr auch ein höchstrichterliches Urteil des Bundesgerichtshofes . Danach verstoßen permanente Bildaufzeichnungen mit einer Dashcam grundsätzlich gegen datenschutzrechtliche Bestimmungen. Eine permanente und anlasslose Aufzeichnung des gesamten Verkehrsgeschehens während der Fahrt sei zur Beweissicherung nicht erforderlich. Vielmehr sei es technisch möglich, nur kurze und anlassbezogene Aufzeichnungen des unmittelbaren Unfallgeschehens anzufertigen. Das könne z. B. dadurch sichergestellt werden, dass das Material dauerhaft in kurzen Abständen überschrieben wird und erst dann dauerhaft gespeichert wird, wenn es zu einer Kollision kommt.

Davon zu trennen ist die weitere Rechtsfrage, ob es ausnahmsweise zulässig ist, datenschutzrechtlich unzulässige Videoaufzeichnungen als Beweismittel in einem Zivilprozess zuzulassen. Diese spezielle Frage hat der BGH im konkret zu entscheidenden Fall bejaht. Zugleich hat das Gericht jedoch auch betont, dass die Aufsichtsbehörden jederzeit die Möglichkeit haben, Verstöße gegen datenschutzrechtliche Bestimmungen mit hohen Bußgeldern zu ahnden.

3 Beschluss des OLG Celle vom 04.10.2017, Az.: 3 Ss (OWi) 163/17

4 BGH, Urteil vom 15.05.2018, Az.: VI ZR 233/17

# 9.3 Videoüberwachung auf der Kartbahn

Gleich zwei Kartbahnen wurden von einem Betreiber rundum mit Videokameras überwacht. Davon waren sowohl Beschäftigte als auch Kunden betroffen – zu Unrecht, wie erst ich und dann auch das zuständige Gericht feststellten.

Auch Tresen und Sitzbereiche überwacht

Eine Eingabe machte mich bereits im Februar 2016 auf die Videoüberwachung auf zwei Kartbahnen aufmerksam. Im Rahmen des aufsichtsbehördlichen Kontrollverfahrens wurden mir Kamerabilder vorgelegt, die zeigten, dass neben der Kartbahn inklusive Leitstand auch der Gastro-Bereich mit Tresen, Sitzecken und Billardtischen erfasst wurde. Die Überwachung diente der Wahrnehmung des Hausrechts, dem Schutz des Personals und der Dokumentation von Einbrüchen.

Als Datenschutzbeauftragten hatte der Kartbahnbetreiber sich selbst ernannt und im Rahmen seiner Vorabkontrolle festgestellt, dass die Kameras keine Persönlichkeitsrechte einschränkten.

## Zu umfassend überwacht, zu lange gespeichert

Überwachung von Beschäftigten nur bei Verdacht auf Straftat

Das sah ich anders und wies in meinem Prüfbericht darauf hin, dass Beschäftigte an ihren Arbeitsplätzen (Leitstand und Tresen) nur dann überwacht werden dürfen, wenn der Verdacht auf eine konkrete Straftat eines bestimmten Beschäftigten besteht und die Videoüberwachung zur Aufdeckung erforderlich ist[1]. Diese Voraussetzungen sind nicht dauerhaft erfüllt, sodass die Arbeitsplätze, an denen sich Beschäftigte für einen längeren Zeitraum aufhalten, von der Erfassung auszunehmen sind.

Besonders hoch einzustufen ist die Schutzbedürftigkeit der Interessen von Betroffenen in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren. Dies trifft auf die für die Kunden eingerichteten Sitzbereiche oder Spieltische besonders zu. Ihre Persönlichkeitsrechte werden durch eine ständige Videoüberwachung erheblich beeinträchtigt, weshalb diese Bereiche ebenfalls von der Überwachung auszunehmen sind.

Betreiber kann nicht DS-Beauftragter sein

Zur Bestellung des Datenschutzbeauftragten stellte ich fest, dass diese wegen der vorliegenden Interessenkollision nichtig ist. Es gilt das Grundprinzip, dass die zu Kontrollierenden nicht selbst die Kontrolle ausüben dürfen. Auch die Speicherdauer von einer Woche wurde von mir als zu lang beanstandet.

Ich gab dem Betreiber der Kartbahnen Gelegenheit, seine Videoüberwachung entsprechend meiner datenschutzrechtlichen Beurteilung neu auszugestalten.

1 § 32 Abs. 1 S. 2 BDSG-alt

## Erfolg vor Gericht – Bußgeld hat Bestand

Dies lehnte der Inhaber zunächst unter dem Hinweis, dass er die Überwachung nur für seine Mitarbeiter durchführen würde und diese informiert seien, ab. Bei Unfällen mit Personenschaden würden die Kunden den Vorfall erst später melden, sodass eine Verkürzung der Speicherdauer nicht möglich sei.

Anordnung zu überwachten Bereichen und Speicherdauer

Da die Information über den Betrieb einer Videoüberwachungsanlage keine Rechtsgrundlage für die Überwachung darstellen kann und Unfälle mit Personenschäden durch die Leitstelle eigentlich gleich bemerkt werden müssten, habe ich u.a. angeordnet, Mitarbeiterbereiche und Erholungsbereiche der Gäste aus den Erfassungsbereichen der Kameras auszunehmen und die Speicherdauer zu begrenzen. Zudem habe ich dem Betreiber aufgegeben, einen Datenschutzbeauftragten zu benennen.

Änderungen, aber keine Verbesserung

Zwar wurde der Inhaber daraufhin tätig, beim Umstellen der Kameras wurde aber einiges „verschlimmbessert“ So wurden zwar Bereiche aus der Erfassung wie gefordert ausgenommen, durch das Verstellen der Kameras gerieten aber andere Erholungsbereiche für Gäste in die Erfassung. Auch nach einem telefonischen Hinweis auf die problematische Neuausrichtung der Kameras reagierte der Inhaber nicht. Daher setzte ich ein Zwangsgeld fest. Zeitgleich leitete ich ein Ordnungswidrigkeitenverfahren ein.

Der Betreiber erhob im Verwaltungsverfahren Klage gegen meine Entscheidung und legte darüber hinaus gegen meinen Bußgeldbescheid Einspruch ein.

Der Bußgeldbescheid wurde letztlich vor dem Amtsgericht Hannover verhandelt. Das Gericht folgte meinem Bescheid und stellte fest, dass der Betreiber durch die Videoüberwachung auf beiden Bahnen unbefugt personenbezogene Daten erhoben und verarbeitet hat. Für jede Bahn wurde ein Bußgeld im vierstelligen Bereich festgesetzt.

Überwachung nur außerhalb der Öffnungszeiten

Der Kartbahnbetreiber gestaltete die Videoüberwachung schließlich so, dass die Kameras künftig nur noch außerhalb der Öffnungszeiten zur Beweissicherung im Fall eines Einbruchs aktiviert sind. So konnte auch auf die Bestellung eines Datenschutzbeauftragten verzichtet werden.

# 9.4 Umfassende Überwachung im Elektronikmarkt

Mit mehr als 1000 Kameras überwachte ein Elektronikmarkt seine Standorte. Bei meiner Prüfung stellte ich fest, dass die Videoüberwachung in mehreren Bereichen unzulässig war. Inzwischen wurden zahlreiche Kameras abgehängt oder verpixelt.

Dem Kunden eines Elektronikmarkts war aufgefallen, dass einer der Kundenparkplätze mit zahlreichen Videokameras bestückt war. Aufgrund seiner Eingabe prüfte ich das Unternehmen mit mehreren Standorten und bat um die Beantwortung von Fragen sowie um Unterlagen zur Videoüberwachung.

Neben dem Zweck der Überwachung wollte ich u.a. wissen, wo Kameras installiert sind und welche Daten diese im Einzelfall über welche Personen erheben. Die Antwort des Unternehmens war mehr als beeindruckend: Aus den vorgelegten Unterlagen war ersichtlich, dass insgesamt 1.220 Kameras installiert waren – zur Wahrung des Hausrechts, zur Prävention vor unbefugtem Zutritt sowie zur Aufdeckung und Aufklärung von Straftaten.

Über 200 Kameras installiert

## Beschäftigte dürfen nicht ständig überwacht werden

Nach einer ersten Durchsicht bat ich das Unternehmen, alle Bereiche, in denen sich Beschäftigte über einen längeren Zeitraum zur Arbeitserledigung aufhalten, während der Betriebszeiten aus der Erfassung auszunehmen. Denn gemäß § 32 Abs. 1 Satz 2 BDSG, kann lediglich der begründete Verdacht auf eine konkrete Straftat ein berechtigtes Interesse an der Überwachung einzelner Beschäftigter darstellen.

Auch Personaleingänge sollten während der Betriebszeit ausgenommen werden. Da das schutzwürdige Interesse der Betroffenen stets dort überwiegt, wo die Intimsphäre berührt ist, musste auch die Überwachung von Umkleiden und Zugängen zu Sanitäranlagen unterbleiben.

Keine Überwachung von Umkleiden und Toiletteneingängen

## Von 1200 auf 400 Kameras

Das Unternehmen zeigte sich sehr kooperativ und übersandte die Dokumentation nach Überarbeitung der Videoüberwachungsanlage erneut – mit jetzt noch ca. 410 Kameras.

Erfasste Bereiche deutlich eingeschränkt

Inzwischen wurden auch die Erfassungsbereiche zahlreicher Kameras deutlich eingeschränkt. Die Beschäftigtenbereiche hinter den Kassen und Beratungstresen wurden ebenso wie Sitzgelegenheiten für Kunden verpixelt. Die Kamerazahl wurde weiter verringert, so dass zukünftig eine umfassende Mitarbeiterüberwachung ausgeschlossen ist.

Das Verfahren war zum Abschluss des Berichtszeitraums noch nicht beendet.

# F.10. Internationaler Datenverkehr

## 10.1 Datentransfer in die USA – Wie sicher ist der Schutzschild?

Im Jahr 2016 wurde das Privacy-Shield-Abkommen zwischen der EU und den USA verabschiedet. Privacy Shield ist Nachfolger des vom Europäischen Gerichtshof (EuGH) für unwirksam erklärten Safe-Harbor-Abkommens und soll ein angemessenes Datenschutzniveau für in die USA übermittelte personenbezogene Daten garantieren. Die Zweifel an der Wirksamkeit von Privacy Shield sind in den vergangenen Jahren allerdings nicht kleiner geworden.

Der EuGH hatte in seinem wegweisenden Safe-Harbor-Urteil klare Vorgaben zu möglichen weiteren Datenschutzabkommen gemacht:

Vorgaben des EuGH zu Abkommen

- Keine unverhältnismäßigen Zugriffe auf personenbezogene Daten durch öffentliche Stellen
- Gewährung ausreichenden Rechtsschutzes für EU-Bürger
- Einrichtung einer unabhängigen Kontrolle über die Einhaltung der zugesicherten Pflichten

### Privacy Shield wird überprüft

Schon die Art. 29-Gruppe (das Vorgänger-Gremium des Europäischen Datenschutzausschusses) kritisierte Privacy Shield angesichts dieser EuGH-Rechtsprechung. Vor allem die anlasslosen, massenhaften Zugriffe der US-Geheimdienste sowie die unklaren bzw. nicht ausreichenden Befugnisse der zur Überwachung dieser Zugriffe eingesetzten Ombudsperson sprächen gegen eine ausreichende Garantie für einen angemessenen Datenschutz in den USA.

Massenhafte Zugriffe der US-Geheimdienste

Diese Kritik war zentrales Thema der ersten jährlichen Überprüfung (Review) des Privacy Shield im September 2017. Der jährliche Review ist in den Verträgen zu Privacy Shield vorgesehen und hat den Zweck folgende Fragen zu klären:

- Funktioniert Privacy Shield in der Praxis?
- Bietet Privacy Shield effektiven Datenschutz?
- Besteht (weiterhin) ein angemessenes Datenschutzniveau?

Kein gemeinsames Ergebnis des ersten Reviews

Für die Überprüfung wurden Fragebögen vorbereitet, Erfahrungsberichte ausgetauscht sowie Beiträge von Unternehmen und Organisationen eingeholt. Die Teilnehmer – nationale Vertreter der Aufsichtsbehörden, Vertreter der EU-Kommission und der zuständigen US-Behörden – diskutierten intensiv die verschiedenen Fragen, Sorgen und Kritikpunkte. Leider kamen sie auch nach zweitägiger Beratung zu keinem gemeinsamen Ergebnis.

Die EU-Kommission teilte schon früh nach dem Ende der Beratungen öffentlich mit, man halte Privacy Shield für eine gut funktionierende Datenschutzgarantie, wenn auch die Handhabung in der Praxis noch verbessert werden könne. Insbesondere gebe es ausreichende Schutzvorkehrungen hinsichtlich staatlicher Eingriffe. Dieses positive Ergebnis aus Sicht der Kommission verwundert nicht, da sie selbst das Abkommen verhandelt und geschlossen hatte.

## Aufsicht sieht weiter grundlegende Mängel

Die Datenschutzaufsichtsbehörden übten demgegenüber keine Zurückhaltung: Zwar erkannten sie die Fortschritte des Privacy Shield gegenüber dem Safe-Harbor-Abkommen an. Grundlegende Mängel bestanden aber aus Sicht der Aufsicht weiterhin.

Insbesondere die massenhaften Zugriffe auf personenbezogene Daten durch US-Geheimdienste seien nicht hinnehmbar und mit dem europäischen Verständnis von Datenschutz nicht vereinbar. Es bestünden nach wie vor keine wirksame Aufsicht und kein effektiver Rechtsschutz für EU-Angehörige in den USA. Die Position der Ombudsperson sei weiterhin nicht dauerhaft besetzt, auch die Befugnisse dieser Stelle seien nach wie vor unklar. Es folgte die unmissverständliche Forderung der Datenschutzaufsichtsbehörden: Das Abkommen muss nachgebessert, die Mängel beseitigt werden.

Wirksame Aufsicht und effektiver Rechtsschutz fehlen

## Was wird aus Privacy Shield?

In der folgenden Zeit war spürbar, welch großes Interesse sowohl die US-Seite als auch die EU-Kommission an einer Beruhigung der Lage und Ausräumung der Kritik hatte. Immer wieder wurden Gespräche gesucht. Dies gipfelte in einem Besuch der kommissarisch tätigen Ombudsfrau in einer Plenumssitzung des Europäischen Datenschutzausschusses, in welcher weiter über die festgestellten Mängel diskutiert wurde.

Währenddessen schaltete sich das EU-Parlament in die Diskussion um Privacy Shield ein und verabschiedete eine Resolution: Privacy Shield solle ausgesetzt werden, der Rechtsschutz genüge offenkundig nicht. Hintergrund waren die Berichte über den Datenskandal um Facebook und Cambridge Analytica, bei der trotz Privacy-Shield-Zertifizierung Daten in unzulässiger Weise ausgetauscht worden waren. Diese politische Erklärung des EU-Parlaments bedeutete eine spürbare Rückendeckung für die Position der Datenschutzaufsichtsbehörden.

EU-Parlament schaltet sich ein

## Neuer Versuch im zweiten Review

Die Aufsichtsbehörden hatten zwischenzeitlich die Entwicklungen zu Privacy Shield erneut bewertet und Mitte 2018 festgestellt, dass die nach dem ersten Review erhobenen Forderungen in Teilen nach wie vor nicht erfüllt waren. Der Europäische Datenschutzausschuss entschied sich dafür, einen erneuten Versuch zur Bereinigung der Streitpunkte in der Ende 2018 anstehenden zweiten jährlichen Überprüfung zu klären.

Diese Entscheidung wurde auch vor dem Hintergrund eines derzeit laufenden weiteren EuGH-Verfahrens zum Datenschutz getroffen. Denn der EuGH prüft gerade die Rechtmäßigkeit der EU-Standardvertragsklauseln, einem weiteren Regelwerk der EU-Kommission zur Übermittlung von personenbezogenen Daten in Länder außerhalb der EU.

Verfahren zu Standardvetragsklauseln

In diesem Verfahren werden dieselben Fragen aufgegriffen, die auch im Zusammenhang mit Privacy Shield immer wieder Thema sind, zum Beispiel die Frage einer ausreichenden Rechtsschutzmöglichkeit für Betroffene. So kann es durchaus sein, dass die Diskussion um die Mängel bei Privacy Shield durch eine wegweisende Entscheidung des EuGH überholt wird. Bedenkt man die bisher geäußerten Stellungnahmen des EuGH zum Datenschutz, etwa im Safe-Harbor-Urteil, ist durchaus fraglich, ob Privacy Shield auf Dauer bestehen bleiben kann.

# F.11. Datenschutz in (Tele-)Medien

## 11.1 Welche Datenschutzregeln gelten seit der DS-GVO für Webseiten?

Mit der Einführung der Datenschutz-Grundverordnung (DS-GVO) haben sich sehr viele praktische Umsetzungsfragen ergeben. Eine Frage mit sehr großer Breitenwirkung ist etwa, welche Datenschutzvorschriften für Betreiber von Webseiten maßgeblich sind. Schließlich gibt es unzählige Webseiten von Unternehmen, Behörden, Verbänden, Vereinen und Privatpersonen. Die deutschen Datenschutzbehörden haben sich hierzu deutlich positioniert.

Was gilt seit Start der DS-GVO datenschutzrechtlich für Webseiten? Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hat mit der Positionsbestimmung vom 26. April 2018 „Zur Anwendbarkeit des Telemediengesetzes (TMG) für nicht-öffentliche Stellen ab dem 25.5.2018“ eine klare Antwort auf diese Frage gegeben.

Positionsbestimmung TMG – Kurzlink: https://t1p.de/TMG

### Gesetzgeber hätten Konfiikt vermeiden können

Ich möchte voranschicken, dass die Positionierung der DSK aus einer Not heraus geboren worden ist. Der Konflikt zwischen der DS-GVO einerseits sowie der europäischen E-Privacy-Richtlinie und den nationalen Datenschutzvorschriften im Telemediengesetz andererseits hätte von vorneherein vermieden werden können:

- erstens vom europäischen Gesetzgeber, wenn es gelungen wäre, dass zeitgleich mit der DS-GVO die E-Privacy-Verordnung in Kraft tritt und
- zweitens vom deutschen Gesetzgeber, wenn er seinem grundsätzlichen Regelungsauftrag zur Anpassung des nationalen Datenschutzrechts an die DS-GVO fristgerecht und vollumfänglich nachgekommen wäre.

Zur E-Privacy-Verordnung siehe auch Seite 39

### Anwendungsvorrang der DS-GVO

Bereits Anfang 2018 war die folgende Situation für Deutschland absehbar: Ab dem 25.5.2018 ist die DS-GVO zwingend anzuwenden. Diese genießt grundsätzlichen Anwendungsvorrang vor nationalen Datenschutzvorschriften. In

Deutschland wird der Datenschutz für elektronische Informations- und Kommunikationsdienste – kurz gesagt alle Webdienste – bereichsspezifisch in den §§ 11 ff. TMG geregelt. Dem stand das Europarecht zuvor auch nicht entgegen.

Seit dem 25.5.2018 hat sich das Verhältnis zwischen europäischen und nationalen Datenschutzvorschriften gewandelt. Die nationalen Datenschutzvorschriften können nur noch angewandt werden, wenn die DS-GVO dem nationalen Gesetzgeber einen Regelungsspielraum lässt und die Vorschriften nicht im Widerspruch zur DS-GVO stehen.

Die DSK führt in der genannten Positionsbestimmung aus, dass sie diese beiden Voraussetzungen in Bezug auf die §§ 11 ff. TMG als nicht gegeben ansieht. Folglich stellt sie klar, dass die Aufsichtsbehörden bundeseinheitlich ab dem 25.5.2018 die Datenschutzvorschriften des TMG nicht mehr anwenden werden. Webseiten müssen daher die datenschutzrechtlichen Anforderungen der DS-GVO erfüllen.

Webseiten müssen Anforderungen der DS-GVO erfüllen

## Verarbeitung zu Werbezwecken nur mit Einwilligung

Ich möchte an dieser Stelle nicht verschweigen, dass die Veröffentlichung dieser Positionsbestimmung ein großes – und leider vor allem negatives – Medienecho hervorgerufen hat. Die Interessenverbände und Unternehmen werteten die Positionsbestimmung vor allem als Angriff auf ihre Geschäftsmodelle, die auf personalisierter und individualisierter Werbung auf Webseiten beruhten. Sie gingen davon aus, dass bisher die Nutzungsdaten der Besucher einer Webseite auf der Grundlage von § 15 TMG grundsätzlich zu Werbezwecken verarbeitet werden durften, es sei denn der Betroffene hat von seinem Widerspruchsrecht gegen die Datenverarbeitung Gebrauch gemacht. Die Anwendung der DS-GVO führt nach Auffassung der DSK grundsätzlich dazu, dass die Verarbeitung zu Werbezwecken, die regelmäßig zur Erstellung umfassender Nutzerprofile führt, nur mit vorheriger Einwilligung der Betroffenen zulässig ist.

Unternehmen fühlen sich angegriffen

In diesem Zusammenhang möchte ich Folgendes klarstellen:
Die Positionsbestimmung der DSK

- entspricht den europäischen Vorgaben der E-Privacy-Richtlinie und berücksichtigt – perspektivisch – bereits die Regelungsvorschläge der E-Privacy-Verordnung,
- schafft für die verantwortlichen Betreiber von Webseiten Rechtssicherheit und
- stellt nicht jeglichen Einsatz von Cookies unter das Einwilligungserfordernis.

Rechtssicherheit für Seitenbetreiber

Darüber hinaus war es mir ein besonderes Anliegen, dass im Anschluss an die Veröffentlichung der Positionsbestimmung von der DSK ein schriftliches und mündliches Konsultationsverfahren von Verbänden und Unternehmen durchgeführt worden ist. Die Ergebnisse dieses Austausches sollen in ein umfassendes Ergänzungspapier zur Positionsbestimmung aufgenommen werden. Die Verabschiedung sowie die Veröffentlichung standen zum Ende des Berichtszeitraumes des vorliegenden Tätigkeitsberichtes jedoch noch aus.

Ergänzung geplant

# 11.2 Datenschutz bei Messenger-Diensten

Es erreichten mich zahlreiche Beratungsanfragen und vereinzelte Beschwerden zum Einsatz von Instant-Messenger-Diensten – allen voran zum am weitesten verbreiteten Dienst WhatsApp. Bei der privaten Kommunikation nicht mehr wegzudenken, nimmt die Nutzung dieses Messengers auch unter Beschäftigten von niedersächsischen Behörden und sonstigen öffentlichen Stellen sowie erst recht in Unternehmen zu. Firmen wie Continental, die den Einsatz von WhatsApp zur betrieblichen Kommunikation explizit verbieten, sind die Ausnahme.

Bereits Installation ist problematisch

Es liegt auf der Hand, dass Apotheken, die die Übermittlung von Rezepten per WhatsApp bewerben und Ärzte, die Krankschreibungen via WhatsApp anbieten, die Vorgaben des Datenschutzrechts nicht beachten. Allerdings ist es für einen Datenschutzverstoß beim Einsatz des Messenger-Dienstes gar nicht erforderlich, dass über diesen sensible personenbezogene Daten übermittelt werden. Bereits die Installation des Dienstes selbst durch Behörden und Unternehmen ist mit den Vorgaben der Datenschutz-Grundverordnung (DS-GVO) nicht in Einklang zu bringen.

Ich habe mehrfach öffentlich betont, dass der Einsatz von WhatsApp durch Behörden, sonstige öffentliche Stellen und Unternehmen zur dienstlichen und betrieblichen Kommunikation gegen datenschutzrechtliche Regelungen verstößt.

Bei der Nutzung von WhatsApp ergeben sich im Wesentlichen vier datenschutzrechtliche Probleme:

Probleme bei der Nutzung von WhatsApp

1. Übermittlung der Kontakte aus dem Adressbuch des Nutzers an WhatsApp.
2. Übermittlung von personenbezogenen Daten in die USA.
3. Nutzung von personenbezogenen Daten durch WhatsApp.
4. Übermittlung der Nutzerdaten an andere Unternehmen des Facebook-Konzerns.

## Rechtsgrundlage für jede Datenübermittlung

Wer WhatsApp einsetzt, muss gewährleisten, dass für die Übermittlung aller in seinem Adressbuch gespeicherten Kontaktdaten eine Rechtsgrundlage vorliegt. Für Personen, die WhatsApp nicht bereits nutzen, ist somit eine Einwilligung erforderlich. Gleiches gilt für die Übermittlung der Nutzerdaten von WhatsApp an andere Unternehmen des Facebook-Konzerns. Auch hier ist eine explizite Einwilligung aller Beteiligten notwendig.

Aus den Nutzungsbedingungen ergibt sich, dass WhatsApp bei der Nutzung personenbezogener Daten insbesondere die Grundsätze der Datenminimierung, der Zweckbindung und der Speicherbegrenzung missachtet. Die Installationseinstellungen entsprechen nicht der Anforderung der Datenschutzfreundlichkeit, so dass gegen den Grundsatz Privacy by Default verstoßen wird.

Verstoß gegen „Privacy by Default"

## Merkblätter für den WhatsApp-Einsatz

Um die zahlreichen Beratungsanfragen zu beantworten, wurden in meiner Behörde drei Merkblätter zum Einsatz von WhatsApp erarbeitet, die auf meiner Website abrufbar sind:

- Merkblatt für die Nutzung von WhatsApp in Unternehmen
- Merkblatt für Verantwortliche zur Nutzung von WhatsApp bei Behörden und sonstigen öffentlichen Stellen in Niedersachsen
- Merkblatt für den Einsatz von WhatsApp an Schulen.

Instant-Messenger-Dienste haben zweifellos viele Vorteile für eine schnelle und multimediale Kommunikation. Allerdings darf der Datenschutz hierbei nicht auf der Strecke bleiben. Jeder sollte daher – auch im eignen Interesse – datenschutzkonforme Messenger-Dienste nutzen.

# 11.3 Schutzranzen-App – riskant oder nützlich?

2018 machte die Schutzranzen-App Schlagzeilen und löste eine datenschutzrechtliche Debatte aus. Die App verspricht mehr Sicherheit für Kinder im Straßenverkehr, indem sie diese frühzeitig digital für Autofahrer sichtbar macht. Da sich aus den Medienberichten Anhaltspunkte ergaben, dass die App nicht datenschutzkonform ist, habe ich ein Kontrollverfahren gegen den in Braunschweig ansässigen Betreiber durchgeführt.

App besteht aus zwei Teilen

Die Schutzranzen-App besteht aus zwei Teilen – aus der Kinder-App sowie aus der Eltern-und Autofahrer-App. Diese können ihre jeweiligen Funktionen nur erfüllen, wenn es für beide Apps Nutzer gibt. Für einige Funktionen ist zudem die Kopplung der beiden Apps erforderlich. Beide wurden sowohl rechtlich als auch technisch eingehend dahingehend überprüft, ob sie die Vorgaben des Datenschutzrechts einhalten.

## Das Kontrollverfahren umfasste dabei im Einzelnen:

Prüfung verschiedener Funktionen

- Installationsprozess der Apps
- Warnwestenfunktion (umfasst die Autofahrerfunktion, die Funktion Digitale Warnweste und in Teilen die Anti-Missbrauchs-Funktion).
- Kopplungsfunktion (umfasst die Anonymitäts- und die Familienfunktion)
- Gut-Angekommen-Funktion
- SOS-Funktion

## Wesentliche Prüfkomplexe

Betreiber bestreitet Anwendbarkeit der DS-GVO

Es wurden neben der sachlichen Anwendbarkeit der Datenschutz-Grundverordnung (DS-GVO), die vom Betreiber der Apps bestritten wurde folgende Punkte überprüft:

- die Zulässigkeit der Verarbeitung einschließlich der Einbindung von Auftragsverarbeitern,
- die Erfüllung der Informationspflichten durch den Verantwortlichen,
- das Erfordernis und gegebenenfalls die Umsetzung der Datenschutz-Folgenabschätzung und
- die Sicherheit der Verarbeitung.

## Ergebnisse des Kontrollverfahrens

Prüfung deckt Mängel auf

Das Kontrollverfahren hat im Wesentlichen zu folgenden Ergebnissen geführt:

- Die Verarbeitung der zunächst personenbezogenen Daten der Kinder ist grundsätzlich rechtmäßig.
- Es erfolgt eine sehr frühzeitige Anonymisierung der Positionsdaten der Kinder, so dass keine Bewegungsprofile erstellt werden.
- Es sind zwei Drittdienstleister eingebunden, ohne dass hierfür die datenschutzrechtlichen Voraussetzungen erfüllt sind.
- Die Informationspflichten werden in Bezug auf die Apps nicht umfassend erfüllt, da sie teilweise Fehlinformationen beinhalten und nicht vollständig sind.
- Es wurden keine den Anforderungen von Art. 35 DS-GVO entsprechende Datenschutz-Folgenabschätzungen vorgenommen.
- Die technischen und organisatorischen Maßnahmen reichten nicht aus, um die Sicherheit der Datenverarbeitung angemessen zu gewährleisten.

## Anordnung von neun Maßnahmen

Um die festgestellten Datenschutzverstöße zu beseitigen, habe ich insgesamt neun Einzelmaßnahmen angeordnet, von denen zwei direkt umgesetzt wurden. Durch die übrigen Einzelmaßnahmen wurde der Anbieter der App aufgefordert,

- die Datenübermittlung an Microsoft (über Azure Service) einzustellen; eine Verarbeitung darf erst wieder erfolgen, wenn ein Vertrag zur Auftragsverarbeitung abgeschlossen ist.
- die Einbindung von Google Maps zu entfernen,
- Altversionen der App aus den App-Stores zu entfernen, da diese nicht den Anforderungen der DS-GVO entsprechen.
- irrelevante Felder und Funktionen innerhalb der App sowie serverseitige Verarbeitung zu entfernen.
- die Transportverschlüsselung auf TLS 1.3 umzustellen.
- die lokale Speicherung der GPS-Historie auf die zuletzt gemeldete Positionsinformation zu reduzieren.
- sicherzustellen, dass nur authentifizierte Nutzer in den Entwicklungsmodus der App wechseln können.

Für diese sieben Maßnahmen ist eine Anordnung ausgesprochen worden. Der Nachweis, dass die Maßnahmen umgesetzt worden sind, ist der Anbieters bis zum Ende des Berichtszeitraumes schuldig geblieben.

# F.12. Technik

## 12.1 Standard-Datenschutzmodell und Prozess zur Auswahl angemessener Sicherungsmaßnahmen

Das Standard-Datenschutzmodell (SDM) ist eine Methode zur Herleitung technisch-organisatorischer Maßnahmen aus den rechtlichen Vorgaben der Datenschutz-Grundverordnung. Es wird gemeinschaftlich von den deutschen Datenschutzaufsichtsbehörden entwickelt und liegt in einer Erprobungsfassung vor. Als ergänzende Praxishilfe zum SDM wurde in meiner Behörde der „Prozess **z**ur **A**us**w**ahl **a**ngemessener **S**icherungsmaßnahmen" (ZAWAS) entwickelt. Dieser soll einer verantwortlichen Stelle die praktische Umsetzung des SDM erleichtern.

In den vorangegangenen Tätigkeitsberichten habe ich das SDM ausführlich dargestellt. Es ist die Grundlage für die Einführung einer einheitlichen Methode zur systematischen Prüfung aller rechtlichen und technisch-organisatorischen Aspekte am Maßstab der Datenschutz-Grundverordnung (DS-GVO).

Mit Blick auf die Geltung der DS-GVO ab dem 25. Mai 2018 wurde die SDM-Version 1.0 vom Oktober 2016 überarbeitet. Die neue Version 1.1 wurde durch die Datenschutzkonferenz im April 2018 verabschiedet. Auch diese ist als Erprobungsversion deklariert, weil weitere Anpassungen notwendig sind. Diese Arbeiten wurden inzwischen aufgenommen, eine Folgeversion wird für 2019 angestrebt.

## ZAWAS: Hilfe für Behörden und Unternehmen

SDM-Version 1.1
ist in der Erprobung

Die DS-GVO stellt hohe Anforderungen an die technisch-organisatorischen Maßnahmen (TOM). So sollen die Rechte und Freiheiten natürlicher Personen bewahrt und die Sicherheit der Datenverarbeitung gewährleistet werden. Die Verantwortlichen stehen daher vor der Herausforderung, ein umfassendes und systematisches Konzept für die datenschutzkonforme Gestaltung von Verarbeitungstätigkeiten zu entwickeln.

ZAWAS – Kurzlink:
https://t1p.de/ZAWAS

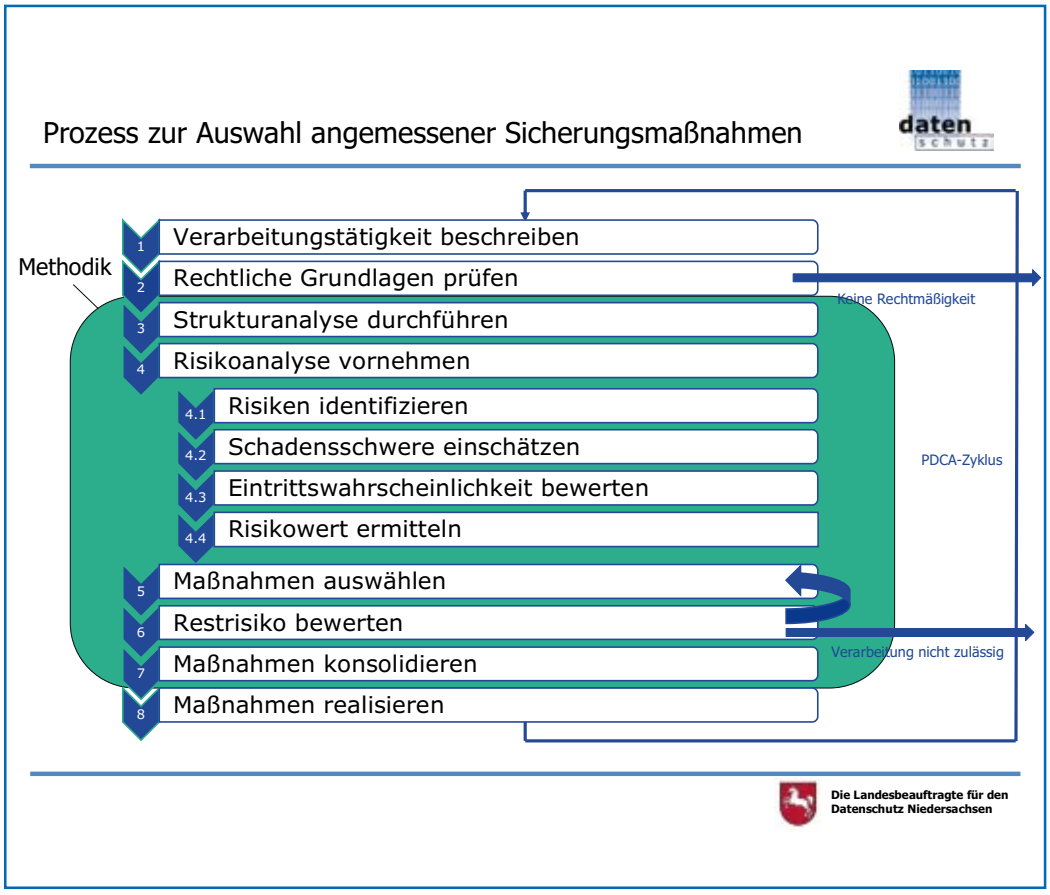
Hierzu bietet der Prozess ZAWAS den Verantwortlichen Hilfe. Er beschreibt eine ganzheitliche Methode, mit der die Anforderungen der DS-GVO zur Ermittlung der geeigneten TOM ordnungsgemäß umgesetzt werden können. Mein Haus hat den Prozess entwickelt, um verantwortlichen Stellen eine Methode aufzugeigen, mit der angemessene Sicherungsmaßnahmen für die Verarbeitungstätigkeiten ausgewählt werden können. Der Prozess ist als Handlungsempfehlung für Praktiker gedacht und sowohl für den Einsatz in Behörden als auch in Unternehmen geeignet. Darüber hinaus ist ZAWAS auch Grundlage für Prüfungen zu TOM durch meine Behörde.

## Nachvollziehbar, belastbar, reproduzierbar

Regelmäßige Evaluation möglich

Das prozessbasierte methodische Vorgehen stellt sicher, dass die gefundenen Lösungen nachvollziehbar, belastbar und reproduzierbar sind. Da es sich nicht um einen einmaligen Vorgang, sondern um einen Prozess handelt, können mögliche Veränderungen bei der Verarbeitungstätigkeit berücksichtigt werden. Zudem ist so eine Orientierung an den aktuellen technischen Rahmenbedingungen möglich. Gleichzeitig können die durchgeführten Maßnahmen regelmäßig evaluiert werden. Der Verantwortliche kann diesen Prozess sowohl bei der Durchführung einer Datenschutz-Folgenabschätzung (DSFA) als auch bei der Absicherung einer Verarbeitungstätigkeit nutzen, für die keine DSFA zu erstellen ist.

Die zentrale Forderung der DS-GVO zur Risiko orientierten Vorgehensweise wird im Prozess ZAWAS berücksichtigt und systematisiert. Dasselbe gilt für die Anforderung zur Gewährleistung angemessener Sicherungsmaßnahmen, die Berücksichtigung der Rahmenbedingungen der Verarbeitung und die Implementierung einer zyklischen und standardisierten Vorgehensweise.



# G. Berichte aus der Behörde

## G.1. Datenschutzinstitut Niedersachsen

Nach wie vor sind die Angebote des Datenschutzinstituts Niedersachsen (DsIN) bei den Beschäftigten des öffentlichen Dienstes sehr gefragt. Neue Kurse waren im Berichtszeitraum meist schnell ausgebucht und die Wartelisten füllten sich. Besonders gut angenommen wurden die Kurse zur Umsetzung der Datenschutz-Grundverordnung.

Umsetzung der DS-GVO sorgt für starke Zunahme der Teilnehmerzahl

Wie in vielen anderen Bereichen meiner Behörde sorgte die Datenschutz-Grundverordnung (DS-GVO) auch im DsIN für eine Steigerung der Anfragen und des Arbeitsaufwandes. Wurden 2017 im Institut noch rund 380 Teilnehmer geschult, waren es 2018 etwa 620. Diese Steigerung lag vor allem am neu eingeführten Kurs „Umsetzung der Datenschutzreform nach der neuen Datenschutz-Grundverordnung“, den mehr als 200 Teilnehmer besuchten. Daneben wurden die Angebote „Basiswissen für behördliche Datenschutzbeauftragte“ und „Datenschutz in Schulen“ besonders gut angenommen. Auch der jährlich stattfindende Erfahrungsaustausch der behördlichen Datenschutzbeauftragten war jeweils bis auf den letzten Platz besetzt.

### Einstellung der Inhouse-Schulungen

Zahlreiche Interessierte konnten meine Mitarbeiterinnen und Mitarbeiter auch wieder in diversen Inhouse-Schulungen erreichen. Darunter waren zum Beispiel Veranstaltungen für die Handwerkskammer Hannover, die Evangelisch-lutherische Landeskirche, das Staatliche Gewerbeaufsichtsamt, das niedersächsische Justizministerium und diverse Kommunen. Zu meinem Bedauern mussten wir diese Inhouse-Schulungen zum zweiten Quartal 2018 einstellen, da das von der DS-GVO verursachte zusätzliche Arbeitsaufkommen dafür keine Kapazitäten mehr ließ. Ob und wann wir dieses Angebot wieder aufnehmen können, steht zum Zeitpunkt dieses Berichts noch nicht fest.

Multiplikator-Effekt noch besser nutzen

Seit jeher ist es unter anderem das Ziel des DsIN, die Teilnehmer zu Multiplikatoren in Sachen Datenschutz zu machen. Sie sollen durch die Kurse in die Lage versetzt werden, das Datenschutzbewusstsein in ihren jeweiligen Behörden oder Stellen zu fördern und ihre Kollegen beim Suchen von praxisnahen Lösungen zu unterstützen. Ich prüfe derzeit, wie sich dieser Multiplikator-Effekt noch verstärken und aktiver von meiner Behörde in die Breite tragen lässt.

# G.2. Bericht aus dem IT-Labor:

## Technische Prüfungen gewinnen an Bedeutung

Häufig senden Internetseiten, Smartphones oder Apps wertvolle Nutzerdaten an die Systembetreiber, ohne dass der Anwender es weiß oder dem zugestimmt hat. Um solche unzulässigen Datenströme verlässlich nachweisen zu können, habe ich im Jahr 2016 in meinem Haus ein IT-Labor aufgebaut, dessen Tätigkeit immer wichtiger wird.

Die zunehmende Vernetzung und Digitalisierung vieler Lebensbereiche ist für die meisten Bürger mittlerweile zu einem täglich genutzten und selbstverständlichen Begleiter im Alltag geworden. Der Einsatz neuer Technologien sorgt für ein Mehr an Funktionalität und Bequemlichkeit. Andererseits bieten viele der neuen Dienste neben dem eigentlichen Zweck der Bedürfnisbefriedigung für den Nutzer auch für Hersteller und Betreiber Vorteile. So senden die verschiedensten Endgeräte, Websites oder Apps wertvolle Nutzerdaten an die Betreiber der Systeme, die diese dann – häufig ohne Kenntnis der Nutzer – in einer zweiten Wertschöpfungskette zu Profilen zusammensetzen und zu Geld machen können. Da dies häufig ohne Einwilligung der Nutzer erfolgt, ist es datenschutzrechtlich unzulässig.

Dass Nutzerdaten an Betreiber oder andere Dritte übermittelt werden, kann in einem Prüf- oder Kontrollverfahren nur durch eine Analyse der Datenströme nachgewiesen und dokumentiert werden. Eine solche Analyse lässt sich sachgerecht nur mit einer technischen Untersuchung unter kontrollierten Laborbedingungen durchführen. Mit dem Ergebnis dieser technischen Prüfung können dann Maßnahmen angeordnet werden, die einen datenschutzkonformen Einsatz der Dienste sicherstellen und den Bürger vor Missbrauch schützen.

Websites und Apps auf den Zahn gefühlt

Nach dem Aufbau und der Inbetriebnahme des IT-Labors 2016 haben sich die Prüftätigkeiten in den Jahren 2017 und 2018 im Wesentlichen auf die Kontrolle von Websites und Smartphone-Apps konzentriert.

### Prüfung von Websites

Bereits vor Einführung der Datenschutz-Grundverordnung (DS-GVO) hatten Website-Betreiber einige datenschutzrechtliche Rahmenbedingungen zu

beachten. Durch die DS-GVO haben sich diese weiter konkretisiert und zum Teil verschärft. Im Rahmen der technischen Prüfung von Websites haben wir unser Augenmerk verstärkt auf die folgenden drei Aspekte gelegt:

### 1. Verschlüsselung

Erhält ein Nutzer auf einer Website die Möglichkeit, über Formulare Eingaben zu machen, z. B. die Bestellung eines Newsletters, eine Kontaktanfrage an den Betreiber oder das Abgeben einer Bestellung in einem Webshop, so werden seine personenbezogenen Daten übertragen und verarbeitet. Damit diese Übertragung sicher erfolgt, muss der Website-Betreiber die Daten bei der Übermittlung, also dem Transport, verschlüsseln. Heutzutage sollte dazu das Übertragungsprotokoll TLS 1.3 verwendet werden, das im Jahr 2018 von den entsprechenden Gremien verabschiedet und freigegeben wurde. In einer Übergangsfrist akzeptiert meine Behörde auch noch den Einsatz der Vorversion TLS 1.2.

Sichere Übertragung durch Verschlüsseln

Im IT-Labor wird überprüft, ob die Websites eine Verschlüsselung einsetzen und ob das Übertragungsprotokoll den Anforderungen entspricht.

### 2. Übermittlung von Daten

Sobald ein Nutzer mit einer Website interagiert, werden Daten an die Seite übermittelt. Häufig werden zudem auf Websites neben den Inhalten des Betreibers auch Dienste von Dritten eingebunden, z.B. Anfahrtskarten durch Google Maps oder Videos durch YouTube. Sobald der Nutzer dann die Website aufruft, werden zusätzlich Daten an die Betreiber der eingebundenen Dienste gesendet. Dabei ist auch zu unterscheiden, ob der Dienstanbieter geografisch im Bereich der DS-GVO ansässig ist, oder ob die Daten an ein Drittland übermittelt und dort verarbeitet werden. Diese Übermittlung muss dem Nutzer in der Datenschutzerklärung der Website angezeigt werden. Durch den Einsatz verschiedener Tools wird im IT-Labor der Datenverkehr analysiert und eine Liste der kontaktierten Server der Dienstanbieter erstellt. Anschließend wird ermittelt, in welchem Land sich der entsprechende Server befindet. In einem weiteren Prüfschritt wird die vorliegende Datenschutzerklärung mit den Erkenntnissen der technischen Prüfung der Website abgeglichen; fehlende Dienste oder falsche Informationen werden gekennzeichnet.

Übermittlung von Daten in Drittländer

Mit diesen Informationen können die juristischen Fachreferate des Hauses dann eine Beurteilung der vorliegenden Website vornehmen und bei Fehlverhalten notwendige datenschutzrechtliche Maßnahmen einleiten.

### 3. Einsatz von Cookies

Viele Website-Betreiber setzen Cookies ein, um ihre Seite zu optimieren. Dazu werden die Informationen in den Cookies ausgewertet und die Website ggf. angepasst.

Cookies zur Finanzierung der Seite

Neben diesen „technischen“ Cookies werden auch häufig Cookies von Drittanbietern eingesetzt, um die Website zu refinanzieren. In diesem Fall werden die Inhalte der Cookies durch den Drittanbieter ausgewertet, indem z.B. Nutzerprofile erstellt werden. Diese Profile werden dann durch den Drittanbieter vermarktet, wofür der Website-Betreiber Geld erhält.

Der Nutzer muss über den Einsatz von Cookies durch ein Pop-Up-Fenster informiert werden und die Möglichkeit erhalten, dem Einsatz von nichttechnischen Cookies zu widersprechen.

Im IT-Labor wird ermittelt, welche Cookies auf der Website eingesetzt werden, welchen Inhalt sie haben und an welchen Empfänger die Daten übermittelt werden. Nach dem Abgleich dieser Informationen mit der Datenschutzerklärung kann festgestellt werden, ob der Website-Betreiber seinen Pflichten nachgekommen ist und die Seite datenschutzkonform betrieben wird. Ist dies nicht der Fall, kann der Verantwortliche aufgefordert werden den Einsatz von Cookies zu unterlassen oder seine Datenschutzerklärung anzupassen.

## Prüfung von Apps für Smartphones

Neben der Prüfung von Websites lag unser zweiter Prüfungsschwerpunkt im Berichtszeitraum auf der Prüfung von Apps für Smartphones.
Apps (Kurzform für Applications) sind ausführbare Programme / Anwendungen, die auf mobilen Endgeräten und PCs installiert werden können. Im Unterschied zu Websites liegt der Programmcode nicht in (für Menschen) lesbarer Form vor. Stattdessen wird vom Anbieter aus dem Quellcode ein maschinenlesbarer Code generiert. Dadurch ist nur mit sehr großem Aufwand zu ermitteln, welche Verarbeitungsschritte eine App ausführt.

Großer Aufwand bei App-Analyse

Aus diesem Grund werden im IT-Labor im Wesentlichen die „Ergebnisse" der Verarbeitung analysiert. Dies sind die lokale Speicherung von Daten auf dem Endgerät, die von der App angeforderten Berechtigungen sowie die Übermittlung von Daten zu verschiedenen Empfängern.

### 1. Lokale Speicherung von Daten auf dem Smartphone

Die Verarbeitung von Daten durch Apps erfolgt im Hauptspeicher des Smartphones. Die Ergebnisse der Verarbeitung werden zum Teil auf dem Speicher des Smartphones abgelegt. Dies findet entweder im Speicherbereich statt, auf den der Nutzer zugreifen kann, oder im systemgeschützten Bereich.
Im IT-Labor haben wir die Möglichkeit, auf beide Speicherbereiche zuzugreifen, die gespeicherten Daten zu analysieren und festzustellen, ob personenbezogene Daten abgelegt werden.

### 2. Von der App angeforderte Berechtigungen

Oft mehr Berechtigungen angefordert als nötig

Da eine App ein eigenständiges Programm auf dem Smartphone ist, nutzt sie für die Verarbeitung häufig vom Betriebssystem des Smartphones bereitgestellte Systemfunktionen und Dienste. Oft werden allerdings mehr Berechtigungen angefordert, als für die eigentliche Funktion benötigt werden (z. B. Berechtigung auf Zugriff des Standortes oder die Kontakte, obwohl diese nicht benötigt werden). Vielfach werden die zusätzlich angeforderten Berechtigungen dafür verwendet, personenbezogene Daten des Nutzers auszulesen und zu übermitteln.

Daher versuchen wir im IT-Labor die kleinste Menge an Berechtigungen zu ermitteln, die notwendig ist, damit der eigentliche Zweck der App dem Nutzer zur Verfügung steht. Berechtigungen, die darüber hinaus von der App angefordert werden, sollten unterbunden werden.

### 3. Übermittlung von Daten

Dieser Punkt der technischen Prüfung ist identisch mit dem Prüfvorgang bei Websites (s.o.). Allerdings müssen die Daten des Smartphones dazu über den Analyserechner geleitet werden, um untersucht und ausgewertet zu werden.