Unterrichtung

Hannover, den 03.09.2018

Die Landesbeauftragte für den Datenschutz Niedersachsen

23. Bericht über die Tätigkeit der Landesbeauftragten für den Datenschutz

Frau
Präsidentin des Niedersächsischen Landtages
Hannover

Sehr geehrte Frau Präsidentin,

hiermit erstatte ich gemäß § 22 Abs. 3 Satz 1 und Abs. 6 Satz 2 des Niedersächsischen Datenschutzgesetzes in der Fassung vom 29. Januar 2002 (Nds. GVBI. S. 22), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Dezember 2012 den 23. Tätigkeitsbericht für die Kalenderjahre 2015 und 2016.

Mit freundlichen Grüßen

Barbara Thiel

(Verteilt am 06.09.2018)

daten
schutz

Die
Landesbeauftragte
für den Datenschutz
Niedersachsen

23. Tätigkeitsbericht 2015–2016

Niedersachsen

23. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2015 – 2016

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 8.: LfD Niedersachsen, Seite 13, 19, 29: Creativ Collection, Seite 53, 55, 68: Fotolia, Seite 81: Pixabay, Seite 86: Quelle: www.niedersachsen.de, alle weiteren: Ingimage

Druck: Druckerei Albert Funke GmbH
Sorststraße 6, 30165 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

Vorwort

Barbara Thiel

Quantensprung, Erdbeben, neue Zeitrechnung – begrifflich wesentlich darunter ging es kaum, als am 25. Mai 2018 die neue Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union Geltung erlangte. Dass eben jene Verordnung bereits zwei Jahre zuvor – am 25. Mai 2016 – in Kraft getreten war, hatte im Zeitraum dieses Tätigkeitsberichts für weit weniger Aufsehen gesorgt – zumindest in einer breiteren Öffentlichkeit.

Für die Aufsichtsbehörden dagegen war bereits mit jenem 25. Mai 2016 eine Zeit des Umbruchs eingeläutet, die eine völlige Neuausrichtung auch meiner Behörde nötig machte. Fortan galt es, einen erheblichen Teil der Aufmerksamkeit und Arbeitskraft auf die Neuerungen zu richten, welche die DS-GVO mit sich bringen würde, ohne die unvermindert wichtigen Aufgaben und Befugnisse nach „alter" Gesetzeslage zu vernachlässigen. Dieser Tatsache ist es auch geschuldet, dass dieser nunmehr 23. Tätigkeitsbericht für die Jahre 2015 und 2016 zu einem verhältnismäßig späten Zeitraum vorliegt.

Das heißt jedoch nicht, dass die in diesem Bericht behandelten Themen an Aktualität eingebüßt hätten. Vielmehr zeigt sich, dass das Grundrecht auf informationelle Selbstbestimmung ganz unabhängig von den gesetzlichen Rahmenbedingungen immer wieder aufs Neue eingefordert und verteidigt werden muss. Dies gilt zum einen angesichts der regelmäßigen Versuche aus der Politik, das (berechtigte) Bedürfnis der Öffentlichkeit nach Sicherheit zu bedienen, indem zum Teil unverhältnismäßig in die Grundfreiheiten des Einzelnen eingegriffen wird. Zum anderen wird dies in Anbetracht der weiterhin rasanten technischen Entwicklung deutlich, die einen stetig wachsenden Datenstrom mit sich bringt.

Dabei kann ich nicht oft genug betonen: Wir Datenschützer stellen uns nicht gegen Sicherheit, Innovation oder Wachstum. All dies sind erstrebenswerte und berechtigte Ziele von Politik und Wirtschaft. Doch die Erfahrung zeigt uns, dass es eines wachsamen Auges und einer mahnenden Stimme der Aufsichtsbehörden bedarf, um den Grundrechten und -freiheiten der Bürgerinnen und Bürger angemessen Ausdruck zu verleihen. Dieser Aufgabe widme ich mich jeden Tag aufs Neue mit ganzer Kraft ebenso wie meine Mitarbeiterinnen und Mitarbeiter. Für ihren stetigen Einsatz für die Belange des Datenschutzes und ihre Bereitschaft, sich an neue Gegebenheiten anzupassen, möchte ich mich an dieser Stelle ganz ausdrücklich bedanken.

Während ich dieses Vorwort schreibe, sind die Arbeiten am Tätigkeitsbericht 2017/18 schon in vollem Gange. Dieser wird letztmalig einen Zeitraum von zwei Jahren umfassen, bevor wir auch mit unseren dann jährlichen Berichten in die neue Zeitrechnung der DS-GVO eintreten.

Management Summary – Das Wichtigste in Kürze

Der wirtschaftliche Wert von Daten nimmt immer weiter zu. So ist es nicht verwunderlich, dass allerorten eine verstärkte Sammelwut zu verzeichnen ist. Das massenweise Zusammentragen, Speichern und Auswerten von personenbezogenen Daten wird durch die Digitalisierung aller Lebensbereiche weiter beschleunigt.
Umso wichtiger ist es, im europäischen und internationalen Datenverkehr zu verlässlichen rechtlichen Grundlagen zu kommen. Im Berichtszeitraum verdeutlichten die Aufhebung des Safe-Harbor-Abkommens mit den USA, die Nachfolgeregelung des Privacy Shield sowie das Inkrafttreten der Europäischen Datenschutzgrundverordnung (DS-GVO), wie sehr sich der Datenschutz im Umbruch befindet.

Bedenken bei Datenübermittlung in die USA

In solchen Umbruchphasen ist es neben ihrer Kontrolltätigkeit eine der wichtigsten Aufgaben der Aufsichtsbehörden, über die neuen rechtlichen Entwicklungen aufzuklären und zu möglichem Anpassungsbedarf zu beraten. Eine anlasslose Prüfung mittelständischer Unternehmen im Nachgang des Safe-Harbor-Urteils des Europäischen Gerichtshofs (EuGH) machte dies überdeutlich. Denn sie zeigte, dass viele Unternehmen trotz der massiven Bedenken, die mit der Übermittlung personenbezogener Daten in die USA einhergehen, oft keinen aktuellen Überblick über ihre Datenströme hatten.
Diese transatlantischen Datentransfers spielten auch bei einer Beratung zu Microsofts „Deutschland Cloud" eine entscheidende Rolle. Die Unklarheiten und Bedenken waren so groß, dass ich der beratenen Behörde empfohlen habe, von einer Nutzung abzusehen – was diese schließlich auch tat.

Wichtige Urteile zu Vorratsdatenspeicherung und BKA

Einen deutlichen Dämpfer erhielten Sicherheits- und Ermittlungsbehörden kurz vor Ende des Berichtszeitraums. Denn mit seinem Urteil vom 21.12.2016 erteilte der EuGH einer allgemeinen und unterschiedslosen Vorratsdatenspeicherung erneut eine deutliche Absage. Ein aus Sicht des Datenschutzes ebenfalls viel beachtetes Urteil fällte das Bundesverfassungsgericht zum Bundeskriminalamt-Gesetz. Zahlreiche Befugnisnormen des Gesetzes seien zwar nicht in Gänze verfassungswidrig, so das Gericht, die Ausgestaltung im Einzelnen verstoße jedoch an zahlreichen Stellen gegen den Grundsatz der Verhältnismäßigkeit. Die Folge für den Gesetzgeber: Er musste nachbessern.

Diesen Bedarf zur Nachbesserung gab es auch mit Blick auf die polizeiliche Telekommunikationsüberwachung (TKÜ). Bereits in früheren Tätigkeitsberichten hatte meine Behörde umfassend zu den erheblichen datenschutzrechtlichen Mängeln bei der TKÜ Stellung genommen. Diese waren Ende 2016 immer noch vorhanden. Die besonders schwer wiegenden Mängel bei der Mandantentrennung, der unzureichenden Protokollierung und der mangelhaften Verschlüsselung der Inhalts- und Verkehrsdaten führten dazu, dass der Betrieb der TKÜ-Anlage auch zum Ende des Berichtszeitraums aus Sicht des Datenschutzes weiterhin rechtswidrig war.

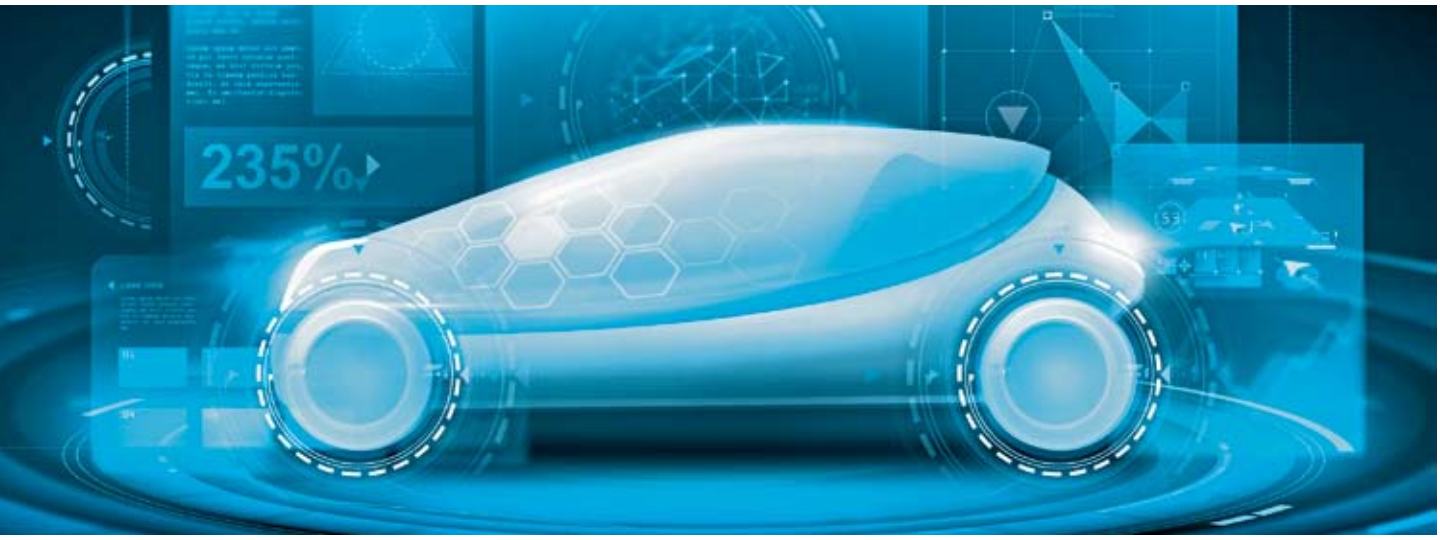
Datenströme in der Schule und beim Sport

Ein Bereich, in dem die Themen Digitalisierung und Datenschutz eine immer größere Bedeutung erhalten, ist die Schule. Dies gilt umso mehr, da es sich bei Schülerinnen und Schülern meist um Jugendliche handelt, deren Daten einem besonderen Schutz unterstehen. Lehrkräfte können durchaus private IT-Geräte nach dem Prinzip „Bring Your Own Device" nutzen. Für deren datenschutzrechtlich akzeptablen Einsatz in der Schule sind allerdings strikte Voraussetzungen einzuhalten. Deshalb habe ich beim Niedersächsischen Kultusministerium (MK) darauf hingewirkt, den Runderlass zur Verarbeitung personenbezogener Daten auf privaten IT-Systemen von Lehrkräften anzupassen. Zudem habe ich das MK im Berichtszeitraum mehrfach darauf hingewiesen, dass eine dienstliche Bereitstellung von IT-Geräten die bessere Alternative darstellen würde.

Auch die tägliche Jogging-Runde kann inzwischen bis ins kleinste Detail nachvollzogen und analysiert werden. So zeichnen sogenannte „Wearables" im Fitnessbereich Gesundheitsdaten und Bewegungsmuster der Trägerinnen und Träger auf und übertragen diese. Häufig geschieht dies jedoch in unnötig großem Umfang und nur unzureichend verschlüsselt, wie eine gemeinsame Prüfung mit anderen Datenschutzaufsichtsbehörden zeigte. Im Ergebnis konnte bei keinem der getesteten Geräte zum Kauf geraten werden.

Datenschutz im Auto

Eine bedeutsame Grundlage für den Datenschutz im Kfz erarbeiteten die Aufsichtsbehörden in Bund und Ländern zusammen mit der Automobilindustrie. In einer gemeinsamen Erklärung wurde ein verbindlicher Standard vereinbart, an dem sich alle Datenverarbeitungsvorgänge im Kfz messen lassen müssen. Der vielleicht wichtigste Punkt darin: Personenbezogene Daten, die im Zusammenhang mit dem Kfz anfallen, gehören dem Fahrer.
Diese Daten sind im Übrigen nicht nur für die Automobilindustrie, sondern auch für die Versicherungsbranche von zunehmendem Interesse. Versicherer bieten verstärkt Telematiktarife an, die schonendes Fahrverhalten goutieren. Im Rahmen einer Beratungsanfrage konnte ich ein niedersächsisches Versicherungsunternehmen von einigen datenschutzrechtlichen Verbesserungsvorschlägen überzeugen.



Videoüberwachung nimmt zu

Ein stets kontrovers diskutiertes Thema ist das der Videoüberwachung, das auch 2015 und 2016 eine gewichtige Rolle gespielt hat. So wurde ich in diesen zwei Jahren allein von öffentlichen Stellen fast 120 Mal beratend hinzugezogen, um eine datenschutzrechtlich einwandfreie Videoüberwachung durchführen zu können.

Problematisch wird es immer dann, wenn für die geplante Überwachung keine Rechtsgrundlage vorliegt. Die niedersächsische Polizei etwa scheint bestrebt, jeden Einsatz bis hin zum täglichen Streifendienst im Bild festzuhalten. Deshalb startete sie im Berichtszeitraum den Einsatz von sogenannten Bodycams - ohne ausreichende rechtliche Grundlage.

Ebenfalls hitzige Debatten löst regelmäßig die Videoüberwachung im öffentlichen Nahverkehr aus. Ihr Ausbau wird stets auch damit gerechtfertigt, dass sie Straftaten verhindere, was aber wissenschaftlich nicht belegt werden kann. Die deutschen Datenschutz-Aufsichtsbehörden äußerten sich im Herbst 2015 in einer Orientierungshilfe ausführlich zu der Frage, unter welchen Voraussetzungen der Videoeinsatz im ÖPNV zulässig ist. Das Ergebnis: Eine uneingeschränkte Überwachung der Fahrgastbereiche kommt datenschutzrechtlich nicht in Betracht.

Vor diesem Hintergrund ist es auch nicht überraschend, dass die Aufsichtsbehörden im November 2016 eine ablehnende Entschließung zum sogenannten Videoüberwachungsverbesserungsgesetz verabschiedeten. Der Gesetzentwurf des Bundesinnenministeriums vermochte nicht zu begründen, dass die angestrebte Erleichterung der Videoüberwachung die öffentliche Sicherheit besser gewährleisten kann, als dies bereits der Fall ist. Zudem lehnte ich es zusammen mit meinen Kolleginnen und Kollegen ab, die Verantwortung für diese Aufgabe auf die privaten Betreiber von Einkaufszentren und öffentlichem Personennahverkehr zu verlagern.

Zu klären war in diesem Zusammenhang auch noch die Frage, ob es sich bei Verkehrsunternehmen überhaupt um private Unternehmen handelt oder ob diese öffentlichen Stellen gleichzusetzen sind. Das Verwaltungsgericht Hannover kam in einem Urteil im Februar 2016 überraschenderweise zu dem Schluss, dass Letzteres der Fall sei, weshalb eine von mir ausgesprochene Anordnung nicht statthaft sei. Ich habe gegen dieses Urteil Berufung eingelegt.

0. Europa und internationaler Datenverkehr

0.1 Europäische Datenschutzreform – Es ist vollbracht

Das Datenschutzrecht steht vor dem Beginn einer neuen Ära: Mit der europäischen Datenschutzreform gibt sich Europa ein einheitliches neues Datenschutzrecht. Die im Jahre 2012 begonnene große Reform des europäischen Datenschutzrechts ist im Jahr 2015 zu einem Abschluss gekommen.

2012: Die Reform nimmt ihren Anfang

Die EU-Kommission leitete im Jahr 2012 mit Vorlage eines Entwurfs für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (RLDSJ) den lang erwarteten Reformprozess des Europäischen Datenschutzrechts ein. Es handelt sich um eine umfassende Rechtsreform, welche die veraltete Datenschutzrichtlinie 95/46/EG von 1995 ablöst. Mit dieser Reform verfolgt die EU folgende Ziele: die Harmonisierung des Datenschutzrechts in Europa durch einen einheitlich gültigen Rechtsrahmen, die Anpassung an neue technische Entwicklungen und die Stärkung des Vertrauens der Bürgerinnen und Bürger in den digitalen Binnenmarkt. Insbesondere die RLDSJ soll dem hohen Bedarf an einem ungehinderten Datenaustausch zwischen den europäischen Strafverfolgungsbehörden entgegenkommen und diesen unter Datenschutzgesichtspunkten regulieren.

2014/2015: Die Reform nimmt Fahrt auf

Nachdem die EU-Kommission 2012 den Startschuss für die Datenschutz-Grundverordnung (DS-GVO) und die RLDSJ gegeben hatte, kam der Reformprozess in Gang. Die ersten Entwürfe der Kommission gaben dabei zunächst Anlass zur Sorge: Können das ausdifferenzierte bereichsspezifische Daten-

schutzrecht sowie das Landesdatenschutzrecht in Deutschland bestehen bleiben? Auch ernteten die Pläne der Kommission, ihre eigenen Kompetenzen auszuweiten, laute Kritik. Insgesamt stand zu befürchten, dass das hohe Datenschutzniveau, wie wir es in Deutschland kennen, durch das neue europäische Recht ausgehöhlt wird.

Von Beginn an begleiteten die Datenschutzaufsichtsbehörden das Gesetzgebungsverfahren aufmerksam und konstruktiv. Da die Kommission für die Regelung des allgemeinen Datenschutzrechts das Rechtsinstrument der Verordnung wählte, ist das neue europäische Recht unmittelbar in Deutschland gültig. Umso wichtiger erschien es daher, dass sich die deutschen Datenschutzaufsichtsbehörden bereits auf europäischer Ebene aktiv für Regelungen einsetzen, die ein weiterhin hohes Datenschutzniveau für Deutschland ermöglichen.

Nachdem zuvor auch das EU-Parlament eigene Ideen in den Entwürfen der DS-GVO und der RLDSJ umsetzte, fanden im Berichtszeitraum dann auch die Verhandlungen der europäischen Innen- und Justizminister des Europäischen Rats statt. Die Vorschläge des Rates zeichneten sich leider dadurch aus, zugunsten wirtschaftlicher Interessen wesentliche Eckpfeiler des Datenschutzes auszuhebeln. Dies zeigte sich zum Beispiel durch Überlegungen zur Aufgabe der Grundsätze der Datensparsamkeit und der Zweckbindung. Auch die Einwilligung als zentrales Instrument des Datenschutzrechts drohte entwertet zu werden. Dieser drohenden Verschlechterung des Datenschutzniveaus galt es insbesondere im Jahr 2015 entgegen zu wirken. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) meldete sich zu diesen Verhandlungen schon frühzeitig zu Wort und mahnte insbesondere mit ihrer Entschließung vom März 2015 an: Die Datenschutzgrundverordnung darf keine Mogelpackung werden!

2015: Das Ziel ist erreicht

In der zweiten Hälfte des Jahres 2015 ging es in die letzte und entscheidende Runde des Gesetzgebungsprozesses: Die Trilogverhandlungen zwischen EU-Kommission, EU-Parlament und Rat der EU. Hier galt es, einen Ausgleich zu finden zwischen den verschiedenen Interessen der an der Gesetzgebung Beteiligten und deren unterschiedlichen Vorschlägen für DS-GVO und RLDSJ.
Zum Beginn dieser entscheidenden Trilogverhandlungen meldete sich die DSK erneut zu Wort und veröffentlichte ihr Papier „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen zur Datenschutz-Grundverordnung" vom 14.08.2015. An dieser Stelle im Verfahren waren die Datenschutzaufsichtsbehörden in besonderer Weise dazu aufgerufen, erneut und sehr deutlich die Erhaltung des bestehenden Datenschutzniveaus einzufordern. Hierzu haben wir die wichtigsten Punkte in der Diskussion um die DS-GVO aufgegriffen und uns dafür eingesetzt, dass weder die zentralen Datenschutzgrundsätze wie Datensparsamkeit und Zweckbindung aufgeweicht werden, noch eine Einschränkung der für die Ausübung des Rechts auf informationelle Selbstbestimmung so wichtigen Betroffenenrechte durch das neue Recht erfolgen darf. Auch sprachen wir uns für eine umfassende Pflicht zur Bestellung eines behördlichen bzw. betrieblichen Datenschutzbeauftragten aus, da dieses Instrument in der Praxis von besonderer Bedeutung für die Etablierung einer Datenschutzkultur in Behörde und Betrieb ist.
Auch im Hinblick auf die RLDSJ sahen wir Handlungsbedarf: Mit dem Papier „Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutzrichtlinie im Bereich von Justiz und Inneres" vom 29.10.2015 brachten wir uns gemeinsam mit der DSK in die Diskussion zum Datenschutz bei Datenverarbeitung durch Polizei und Justizbehörden im Zusammenhang mit Strafverfolgung ein. Da es zuvor in diesem Bereich keine eigene datenschutzrechtliche Regelung gab, begrüßten wir ausdrücklich den Gesetzentwurf einer solchen Richtlinie aus dem europäischen Raum. Auch hier galt es jedoch, wichtige Datenschutz-Prinzipien zu verteidigen. Keine Aufweichung des Zweckbindungsgrundsatzes, besonderer Schutz für Unverdächtige wie Zeugen oder Opfer, umfassende Benachrichtigungspflichten, mehr Befugnisse für die Datenschutzaufsichtsbehörden.
Zum Ende des Jahres 2015 lagen dann mit dem Abschluss der Trilogverhandlungen die endgültigen Gesetztestexte für DS-GVO und RLDSJ vor. Mit der Veröffentlichung der neuen Regelungen im EU-Amtsblatt am 04.05.2016 wurde die große Reform des Datenschutzes abgeschlossen.
Der europäische Gesetzgeber gewährt allen Beteiligten eine Umsetzungsfrist der neuen DS-GVO von zwei Jahren, so dass diese am 25.05.2018 in Kraft treten wird.
Nach fast vier Jahren Arbeit am Reformprozess ist damit das große Ziel erreicht: Europa hat ein neues Datenschutzrecht. Aus heutiger Sicht ist es erfreulich, dass eine so umfassende Reform in der EU möglich war und alle Interessen weitgehend in Einklang gebracht werden konnten.

Eine Verordnung für den Datenschutz in Europa

Für den Bereich des allgemeinen Datenschutzrechts gilt fortan die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr zur Aufhebung der Richtlinie 95/46/EG (DS-GVO). Das Regelungsinstrument der Verordnung hat die Harmonisierung des Datenschutzrechts in der EU durch eine direkte Anwendung desselben Rechts in ganz Europa zur Folge. Dies war ein erklärtes Ziel der EU-Kommission. Künftig können sich die Unternehmen in Europa für die Festlegung ihres Unternehmenssitzes nicht mehr einen Mitgliedstaat mir geringerem Datenschutzniveau auswählen, da das neue Datenschutzrecht überall gilt. Auch die

vielen Öffnungsklauseln, welche die DS-GVO enthält, ändern an diesem grundlegenden Prinzip nichts. Obwohl es möglich und auch vorgesehen ist, dass die Mitgliedstaaten eigene Regelungen zu speziellen Bereichen des Datenschutzrechts treffen, hat die DS-GVO doch als gemeinsame Rechtsbasis Geltung für alle Staaten der EU.
Die DS-GVO bringt uns einige wesentliche neue Regelungen. Das neu eingeführte Marktortprinzip führt dazu, dass das europäische Datenschutzrecht auch von außerhalb der EU niedergelassenen Unternehmen zu beachten ist, wenn diese ihre Waren oder Dienstleistungen innerhalb der EU anbieten. In Zukunft können Unternehmen und betroffene Personen Beschwerden an die Datenschutzbehörde in ihrem eigenen Mitgliedstaat richten, unabhängig davon, wo die für die Datenverarbeitung verantwortliche Stelle ihren Sitz hat (One-Stop-Shop). Informationsrechte der betroffenen Personen und Dokumentationspflichten der verantwortlichen Stellen sind erweitert worden. Das so genannte „Recht auf Vergessen" verpflichtet die verantwortliche Stelle, auf Verlangen einer betroffenen Person zu einer umfassenden Löschung ihrer personenbezogenen Daten im Internet hinzuwirken. Insbesondere zum Schutz Minderjähriger finden sich neue Regelungen, z.B. bezüglich der Einwilligung in die Datenverarbeitung bei Nutzung von Internet-Dienstleistungen. Das neue Datenschutzrecht zeichnet sich auch durch erheblich schärfere Sanktionsmöglichkeiten aus, so ist der Bußgeldrahmen deutlich erhöht worden. Die Anpassung an neue Technologien zeigt sich in den neuen Grundsätzen Privacy by Design und Privacy by Default – Datenschutz soll schon bei der Herstellung von Waren und bei der Konzipierung von Dienstleistungen eine Voraussetzung sein. Neue Zertifizierungsmöglichkeiten ergänzen die bisherigen Datenschutzregelungen. Künftig wird es möglich sein, auch gegen öffentliche Stellen Anordnungen bei Datenschutzverletzungen zu erlassen. Zur Umsetzung des Ziels der einheitlichen Anwendung des neuen Rechts in allen EU-Mitgliedstaaten dienen detaillierte Regelungen zur verpflichtenden Zusammenarbeit der Aufsichtsbehörden bei Datenverarbeitungen mit europaweiter Bedeutung (Kohärenzverfahren). Auch der neu eingerichtete Europäische Datenschutzausschuss soll die Zusammenarbeit der Aufsichtsbehörden und die einheitliche Rechtsauslegung sicherstellen.
Im Gesetzgebungsverfahren wurden einige der Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgegriffen. So konnte eine weitere Aufweichung der Datenschutzgrundsätze der Datensparsamkeit und der Zweckbindung verhindert werden, die Einwilligung behält ihren bisherigen Charakter und auch das Instrument der behördlichen bzw. betrieblichen Datenschutzbeauftragten bleibt erhalten.
Die zahlreichen Öffnungsklauseln und Regelungsgebote in der DS-GVO bieten Gestaltungsmöglichkeiten für die einzelnen Mitgliedstaaten auf Basis der Regelungen der DS-GVO. So ist es zum Beispiel möglich, eigene nationale Regelungen im Bereich öffentlicher Aufgaben zu treffen, auch die Datenschutzgesetze der Länder können so erhalten bleiben. Es bestehen Regelungsaufträge, z.B. zur Errichtung der Aufsichtsbehörden in den Mitgliedstaaten, und Regelungsbefugnisse, z.B. zum Beschäftigtendatenschutz. Durch diese Konstruktion können nationale Besonderheiten und auch Errungenschaften im Datenschutz erhalten bleiben, dabei bildet die DS-GVO eine starke einheitliche rechtliche Grundlage.

Eine Richtlinie für Polizei und Justiz

Die Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (RLDSJ) gilt ausschließlich für den Bereich Justiz und Inneres. Da es sich hier um das Rechtsinstrument der Richtlinie handelt, sind ihre Regelungen in eigenes Recht in den Mitgliedstaaten umzusetzen.

Anders auch als bei den Öffnungsklauseln der DS-GVO hat der nationale Gesetzgeber hier weitgehende Spielräume bei der Umsetzung in eigene Regelungen. Dahinter steht der Gedanke, die unterschiedlichen Rechtstraditionen in den einzelnen Mitgliedstaaten zu respektieren, aber auch klare Grundregeln vorzugeben.
Die RLDSJ gibt erstmals Regelungen zum Austausch personenbezogener Daten zwischen Polizei- und Justizbehörden in der EU vor. Des Weiteren finden sich hier grundlegende zu beachtende Prinzipien wie Datensparsamkeit und Verhältnismäßigkeit. Die Aufsicht über diese Datenverarbeitungen ist erstmals geregelt. Außerdem erhält der Rechtsschutz der betroffenen Personen nun Ausdruck im Gesetz.

Ist die Reform gelungen?

Die Ziele, welche die EU-Kommission mit der Datenschutzreform verwirklichen wollte, konnten größtenteils erreicht werden. Die DS-GVO wirkt vereinheitlichend und harmonisierend auf die unterschiedlichen Datenschutzstandards in den einzelnen EU-Mitgliedstaaten. Auch die technische Entwicklung hat zumindest teilweise Eingang in das neue Recht gefunden. Insgesamt ist der Datenschutz auch im digitalen Binnenmarkt gestärkt worden.
Die Datenschutzreform ist letztlich als Erfolg zu werten. In ganz Europa herrscht künftig ein einheitlich hohes Datenschutzniveau durch das Rechtsinstrument der Verordnung und durch die verbindlichen Regelungen zur Zusammenarbeit der Aufsichtsbehörden. Das veraltete Datenschutzrecht aus den neunziger Jahren wurde an moderne Technologien und Geschäftsfelder angepasst, der Ausgleich zwischen der freien Entfaltung des digitalen Binnenmarktes und der Weitergeltung der bewährten Datenschutzstandards auch in den neuen Geschäftsfeldern scheint gelungen. In diesem Zusammenhang ist auch von Bedeutung, was gerade nicht mit der Reform geändert wurde. So wurden z.B. die tragenden Prinzipien des Datenschutzrechts wie der Grundsatz des Verbots mit Erlaubnisvorbehalt, Zweckbindungsprinzip, Datensparsamkeit aufrecht erhalten. Datenschutz kann so sogar zu einem Wettbewerbsvorteil werden, etwa durch die in Europa künftig geltenden Grundsätze des Privacy by Design und Privacy by Default und die damit einhergehenden Möglichkeiten zur Zertifizierung von datenschutzkonformen Verfahren und Produkten. Auch die RLDSJ ist positiv zu bewerten: Durch konkrete Regelungen zum Datenschutz bei einem Datenaustausch bei der Strafverfolgung wird letztlich die grenzüberschreitende Zusammenarbeit bei der Bekämpfung von Kriminalität und Terrorismus in Europa erleichtert.

Umsetzung

Mit dem Abschluss des europäischen Gesetzgebungsprozesses begann im Jahr 2016 die Arbeit in den Mitgliedstaaten an der Umsetzung der neuen Rechtsakte. Die Regelungsaufträge und Öffnungsklauseln der DS-GVO sind auszufüllen und die RLDSJ ist in nationales Recht umzusetzen.
Im August 2016 wurde der erste Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung und zur Umsetzung der RLDSJ (Datenschutz-Anpassungs- und Umsetzungsgesetz EU – DSAnpUG-EU) bekannt. Dieses Gesetz soll das bisher geltende Bundesdatenschutzgesetz (BDSG) ablösen. Die neuen Regelungen zur Umsetzung werden hier in einem neuen Datenschutzgesetz auf Bundesebene, im ersten Entwurf mit dem Titel Allgemeines Bundesdatenschutzgesetz zusammengefasst. Dieses neue Gesetz enthält wie das aktuell geltende BDSG Regelungen für die öffentlichen Stellen des Bundes und für den nicht-öffentlichen Bereich.

Konkret werden in diesem Gesetz z.B. die Zulässigkeitsvoraussetzungen für Datenverarbeitungen im öffentlichen Interesse, Betroffenenrechte, die Pflicht zur Bestellung eines behördlichen bzw. betrieblichen Datenschutzbeauftragten, die Ausgestaltung der Aufsichtsbehörden und die Ausgestaltung des Verfahrens zur Verhängung von Geldbußen geregelt.
Mit dem Papier „Datenschutzrechtliche Eckpunkte zu den in die Öffentlichkeit gelangten Überlegungen des Bundesministerium des Innern für ein Gesetz zur Anpassung des Datenschutzrechts an die Datenschutzgrundverordnung und zur Umsetzung der Richtlinie (EU) 2016/689 (Datenschutzanpassungs- und Umsetzungsgesetzes EU – DSAnpUGEU)“ vom 22.09.2016 nahm die DSK in einer Sondersitzung bereits Stellung zu diesem ersten Gesetzentwurf. Es war von besonderer Bedeutung, sich hier frühzeitig in die Diskussion um die Entwicklung eines neuen Bundesdatenschutzgesetzes einzubringen, denn der vorliegende Gesetzesentwurf konnte so nicht akzeptiert werden. Die DSK mahnte unter anderem Folgendes an: Es bedarf einer klaren Trennung zwischen der Umsetzung der Regelungsaufträge und -optionen nach der DS-GVO und der Umsetzung der RLDSJ. Das Gesetz ist zudem sprachlich klarer zu formulieren und insgesamt verständlicher und lesbarer zu verfassen. Kritisiert wurde inhaltlich vor allem die zu weitgehende Einschränkung der Betroffenenrechte, die Aufweichung des Zweckbindungsgrundsatzes und des Grundsatzes der Verhältnismäßigkeit bei der Datenverarbeitung durch öffentliche Stellen sowie die datenschutzrechtliche Besserstellung von Berufsgeheimnisträgern.
Ende 2016 wurde dann ein nachgebesserter Entwurf eines neuen Bundesdatenschutzgesetzes (nun auch unter diesem Namen) bekannt. Wenn auch einigen Forderungen der DSK in diesem Gesetz nachgekommen wurde, wie einer klaren Trennung zwischen den Bereichen Umsetzung der DS-GVO und Umsetzung der RLDSJ, bleiben inhaltlich doch wichtige Kritikpunkte bestehen. Besonders die offenkundige Verabschiedung des Regel-Ausnahme-Prinzips bei einer Verarbeitung von besonderen Kategorien personenbezogener Daten und bei der Verarbeitung zu einem anderen Zweck durch eine Vielzahl an Ausnahmetatbeständen ist nicht hinnehmbar. Es ist von hoher Bedeutung, sich in diesem Gesetzgebungsprozess weiter für den Datenschutz einzusetzen.
Auch in Niedersachsen ist die Datenschutzreform umzusetzen: Die niedersächsischen Gesetze sind dahingehend zu überprüfen, ob sie mit den Regelungen der Grundverordnung übereinstimmen, und ggf. zu ändern bzw. anzupassen. Zumindest das Niedersächsische Datenschutzgesetz ist umfangreich zu überarbeiten. Auch in diesem Gesetzgebungsprozess bin ich laufend eingebunden.

Auswirkungen

In Deutschland besteht bereits ein relativ hohes Datenschutzniveau, es wird daher hier weniger Veränderungen geben als in anderen Mitgliedstaaten der EU. Unternehmen, die bisher schon ihre Hausaufgaben im Bereich Datenschutz gemacht haben, haben auch mit dem Wirksamwerden der DS-GVO weniger Anpassungen vorzunehmen. Kleinere Unternehmen werden sogar entlastet, weil zum Beispiel die bisherige Meldepflicht bei bestimmten Verarbeitungssituationen entfällt.
Durch die Aufwertung des technischen Datenschutzes, etwa durch die nun verbrieften Grundsätze Privacy by Design und Privacy by Default, liegt das Augenmerk im Datenschutz künftig verstärkt auf der technischen Infrastruktur bei Datenverarbeitungen. Schon von Beginn an ist bei jeder Datenverarbeitung mehr auf den Datenschutz zu achten. Diese gesetzlichen Vorgaben bieten sogar die Möglichkeit für deutsche und europäische Unternehmen, hieraus einen Wettbewerbsvorteil im globalen Markt zu ziehen.
Auch die nun vorgegebenen Möglichkeiten, eine datenschutzrechtliche Zertifizierung zu erlangen, können als Wettbewerbsvorteil für EU-Unternehmen genutzt werden.

Für die Betroffenen entsteht mit der DS-GVO mehr Transparenz durch die weitergehenden Informations- und Dokumentationspflichten in den Daten verarbeitenden Unternehmen. Hierdurch kann mehr Vertrauen der Betroffenen beim Umgang mit ihren personenbezogenen Daten entstehen, gerade auch im Bereich neuer Technologien.
Für die Datenschutzaufsichtsbehörden bedeutet diese Rechtsreform, dass neue Aufgaben hinzukommen und dadurch auch deutliche Mehraufwände für die Beschäftigten entstehen. Die DS-GVO sieht zum Beispiel die gesetzlich normierte Pflicht zu verstärkter Öffentlichkeitsarbeit sowie proaktiver Information und Beratung vor. Weiter enthält die DS-GVO das neue Instrument der Datenschutzfolgenabschätzung, bei welcher Unternehmen zu bestimmten besonders risikoreichen Datenverarbeitungen eine umfangreiche Bewertung der Aufsichtsbehörde vorab beantragen können.
Es bestehen auch erweiterte Koordinierungserfordernisse mit den anderen deutschen und europäischen Aufsichtsbehörden, nicht nur wegen der gebotenen einheitlichen Auslegung der Rechtsbegriffe der DS-GVO, sondern auch wegen des neu eingeführten Prinzips des One-Stop-Shop und des vollkommen neuen Kohärenzverfahrens. Immer dann, wenn von einer Entscheidung über eine Datenverarbeitung nicht nur ein Mitgliedstaat betroffen ist, ist das Kohärenzverfahren durchzuführen. Dies bedeutet, dass eine Abstimmung über die Bewertung bzw. Entscheidung der betroffenen Aufsichtsbehörden gemeinsam herbeizuführen ist. Gerade an diesem neu eingeführten Verfahren der Zusammenarbeit der Aufsichtsbehörden in den verschiedenen Mitgliedstaaten zeigt sich einmal mehr der „europäische Gedanke". Für die unabhängigen Aufsichtsbehörden bedeutet dies aber auch eine große Umstellung in der täglichen Arbeit, wenn Entscheidungen nicht mehr ohne Einbindung der anderen betroffenen Aufsichtsbehörden getroffen werden können.
Weitere neue Aufgabenfelder sind das Zertifizierungsverfahren; neue Zuständigkeiten entstehen durch das Marktortprinzip; die Mitwirkung im neuen Europäischen Datenschutzausschuss und seiner Arbeitsgruppen werden Mehraufwände mit sich bringen.
Insgesamt und übergreifend werden die Aufsichtsbehörden für eine längere Zeitspanne verstärkte Kontrollen zur Durchsetzung des neuen Rechts durchführen. Auch die verschärfte Sanktionierung wird Auswirkungen auf den Arbeitsaufwand in den Aufsichtsbehörden haben, ebenso wie die neu geschaffene Möglichkeit, Anordnungen gegenüber öffentlichen Stellen auszusprechen.
Die DS-GVO sieht ausdrücklich vor, dass die Mitgliedstaaten für die Erfüllung ihrer zahlreichen, auch neuen Aufgaben ausreichende personelle, technische und finanzielle Ressourcen zur Verfügung stellen müssen.

Bereit machen

In den nächsten Monaten müssen sich nun alle Betroffenen auf die neuen Gesetzeswerke vorbereiten. Und ab Mai 2018 gilt es dann, die neuen Regelungen mit Leben zu erfüllen. Wir werden tatkräftig daran mitarbeiten – durch vermehrte Beratung und Information, durch verstärkte Kontrollen und eine gemeinsame Auslegung der neuen Regelungen auf der europäischen Ebene.

0.2 Datentransfer in die USA nach dem Safe Harbor-Urteil: Wie halten es die Unternehmen?

Mit dem Ende des Jahres 2015 änderte sich einiges für Unternehmen, die personenbezogene Daten in die USA übermitteln. Der übliche rechtliche Weg über das Safe Harbor-Abkommen verlor seine Wirksamkeit unmittelbar mit dem Datum der Verkündung der Entscheidung des Europäischen Gerichtshofs (EuGH). Die Unternehmen sahen sich nun sehr kurzfristig mit der Aufgabe konfrontiert, ihren elektronischen Datenverkehr mit den USA auf eine andere gültige Rechtsgrundlage zu stützen oder gänzlich einzustellen. Dies war für mich Anlass zu einer aufsichtsbehördlichen Prüfung, inwieweit die Unternehmen ihren rechtlichen Verpflichtungen an dieser Stelle nachgekommen waren.

Das Ende von Safe Harbor

Der EuGH hat am 06.10.2015 die so genannte Safe Harbor-Entscheidung der EU-Kommission aufgehoben. Dieses Abkommen war bisher die zentrale Rechtsgrundlage für den Transfer personenbezogener Daten in die USA. US-Unternehmen konnten über eine inhaltlich nicht überprüfte Selbstzertifizierung Daten aus Europa importieren. Das Instrument Safe Harbor wurde von vielen Unternehmen als attraktive Lösung, die einfach, günstig und rechtssicher war, genutzt. Der EuGH entschied nun, dass die Entscheidung der EU-Kommission keine hinreichenden Feststellungen zu dem tatsächlich in

den USA bestehenden Datenschutzniveau getroffen habe. Dabei hat der EuGH vor allem die anlasslosen Zugriffe US-amerikanischer Behörden auf die übermittelten personenbezogenen Daten und die fehlenden Rechtsschutzmöglichkeiten von EU-Bürgern kritisiert.

Datenübermittlungen in die USA geraten in den Fokus

Im Laufe des Jahres 2016 ging meine Behörde dann der Frage nach, ob und wie die Unternehmen auf das Safe-Harbor-Urteil reagiert hatten. Waren sich die Unternehmen der rechtlichen Auswirkungen des Urteils überhaupt bewusst? Wurden Anpassungen bzw. Änderungen im Geschäftsmodell oder in der Auswahl der Vertragspartner vorgenommen?
Im Juni 2016 fand deshalb eine anlasslose Prüfung von zufällig ausgewählten mittelständischen Unternehmen des sekundären Wirtschaftssektors mittels Fragebögen statt. Die Unternehmen wurden zur Auskunft dazu aufgefordert, ob sie überhaupt personenbezogene Daten in die USA übermitteln, welche Daten übermittelt werden und zu welchem Zweck die Übermittlung erfolgt sowie auf welcher Rechtsgrundlage diese Übermittlungen beruhen.

Bewusstsein schärfen für „versteckte" Datenübermittlungen

Die Prüfung zeigte zunächst, dass die Unternehmen große Schwierigkeiten hatten, überhaupt die konkret geforderten Auskünfte zu erteilen. Viele waren nicht in der Lage, in einer angemessenen Frist genaue Angaben machen zu können, sondern mussten selbst eigene Prüfungen im Unternehmen anstrengen. Auch herrschte in vielen Unternehmen kein Bewusstsein darüber, dass auch im Rahmen von Webseiten-Analysen oder Webseiten-Gestaltung oder bei bestimmten Dienstleistungen wie Cloud Computing oder die Nutzung von Datenverarbeitungsprogrammen von US-Anbietern personenbezogene Daten in die USA übermittelt werden. Hier war viel Aufklärungsarbeit zu leisten. Durch die einfache Gestaltung von Safe Harbor hatten viele Unternehmen über die rechtlichen Grundlagen für ihren Datentransfer gar nicht erst nachgedacht.

Kein Umdenken nach dem Safe Harbor-Urteil

Im Ergebnis fand nur bei einer geringen Anzahl der geprüften Unternehmen keine Datenübermittlung in die USA statt, diese Unternehmen nutzten für bestimmte Dienstleistungen wie Cloud Computing und Webseiten-Analyse ausschließlich deutsche bzw. europäische Vertragspartner. Die überwiegende Zahl der geprüften Unternehmen übermittelt weiterhin personenbezogene Daten in die USA, wobei als Rechtsgrundlage vor allem die EU-Standardvertragsklauseln genutzt wurden. Keines der Unternehmen erklärte, es habe aufgrund des Safe-Harbor-Urteils seine Praxis der Datenübermittlungen in die USA angepasst.

Leider zeigt die durchgeführte Prüfung, dass viele Unternehmen trotz der massiven Bedenken, die mit Übermittlung personenbezogener Daten in die USA für den Datenschutz einhergehen, oft keinen aktuellen Überblick über von ihnen tatsächlich betriebene Transfers haben. Ferner betrachte ich es als unerlässlich, dass die für die Daten verantwortlichen Stellen über das gesetzlich geforderte Mindestmaß hinaus zusätzliche Absicherungen z.B. durch Anonymisierung, Verschlüsselung oder die Nutzung europäischer Dienstleister bei der Umsetzung ihrer Geschäftsmodelle vorsehen. Dies gilt insbesondere im Hinblick auf eine langfristigen Rechtssicherheit für Unternehmen, da die Nutzung der EU Standardverträge unter denselben Defiziten leidet wie die Safe Harbor oder Privacy Shield Vereinbarungen und daher ebenfalls Gefahr laufen, demnächst vom EuGH für unwirksam erklärt zu werden.
Das Thema wird mich daher sicher auch in den nächsten Jahren weiter beschäftigen.

1. Polizei und Verfassungsschutz

1.1 Vorratsdatenspeicherung – Aktuelle Entwicklungen, neues Gesetz der Großen Koalition und Urteil des EuGH aus 2016

Seit 2006 gibt es in Deutschland und Europa eine heftige rechtspolitische und datenschutzrechtliche Debatte zum Thema Vorratsdatenspeicherung (VDS). Demzufolge war die VDS in den vergangenen Jahren regelmäßig Gegenstand in den Tätigkeitsberichten.

Die VDS greift massiv in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen ein. Mit ihr werden die Anbieter von Telekommunikationsdiensten verpflichtet, für eine bestimmte Zeit alle Verkehrsdaten elektronischer Kommunikationsvorgänge zu speichern, ohne dass ein Anfangsverdacht für eine Straftat oder eine konkrete Gefahr besteht. Hierbei werden nicht die Inhalte der Kommunikation erfasst, sehr wohl aber die Verbindungsdaten bei der Nutzung von Internet und Telefon, also Art der Daten, Dauer der Verbindung, Standortdaten der Gesprächspartner.

Ein kurzer Blick in die Vergangenheit

Die Europäische Union hatte unter dem Eindruck der Anschläge in Madrid und London eine Richtlinie über die Vorratsdatenspeicherung am 15.03.2006 verabschiedet, welche Deutschland durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21.12.2007 umgesetzt hatte. Das Bundesverfassungsgericht hat mit Urteil vom 02.03.2010 die Verfassungswidrigkeit dieses Gesetzes festgestellt und damit das Recht auf informationelle Selbstbestimmung als Bestandteil des Persönlichkeitsrechts gestärkt. Damit war die VDS in Deutschland zunächst gescheitert.

Zudem erklärte der Europäische Gerichtshof (EuGH) mit dem Digital-Rights-Urteil vom 08.04.2014 die Richtlinie rückwirkend für unwirksam. Der durch die Richtlinie bedingte schwerwiegende und unverhältnismäßige Eingriff in die Grundrechte stelle einen Verstoß gegen Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union dar. Die Bekämpfung des internationalen Terrorismus sowie die Bekämpfung schwerer Kriminalität sei zwar eine

„dem Gemeinwohl dienende Zielsetzung der Union“, so die Richter des EuGH. Eine VDS sei daher in bestimmten Fallkonstellationen durchaus möglich. Diese müsse jedoch dem Grundsatz der Verhältnismäßigkeit genügen und sich damit „auf das absolut Notwendige“ beschränken.

Aktuelle Entwicklungen: Neues Gesetz der Großen Koalition und Urteil des EuGH aus 2016

Obwohl nach der Aufhebung der Richtlinie durch den EuGH für Deutschland keine unionsrechtliche Verpflichtung mehr bestand, eine Regelung zur VDS zu erlassen, setzte schnell eine politische Diskussion ein, die das Ziel einer nationalen Rechtsgrundlage für die Kriminalitätsbekämpfung mittels Vorratsdatenspeicherung hatte. Hierbei wurde insbesondere argumentiert, dass ein solches Gesetz besonders für Delikte im Internet und mit Hilfe des Tatmittels Internet sowie für schwere Straftaten unverzichtbar sei.

Die Große Koalition aus CDU/CSU und SPD beschloss das „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ vom 10.12.2015, das am 18.12.2015 in Kraft trat. Hiernach haben Telekommunikationsunternehmen ohne jede Ausnahme die gesetzliche Pflicht, die Internetverbindungsdaten und Telekommunikationsmetadaten für zehn Wochen sowie Standortdaten der Mobilkommunikation für vier Wochen zu speichern. Es bedarf, außer bei Gefahr im Verzug, einer vorher erteilten richterlichen Anordnung zur Herausgabe der Daten an die Behörden der Strafverfolgung oder Gefahrenabwehr. Spätestens zum 01.07.2017 sind die Speicherpflichten seitens der Unternehmen zu erfüllen.

Gegen das Gesetz sind bereits mehrere Verfassungsbeschwerden beim Bundesverfassungsgericht eingereicht worden. Eine Entscheidung steht noch aus.

Mit Urteil vom 21.12.2016 hat der Europäische Gerichtshof sich aufgrund von britischen und schwedischen Vorlageersuchen mit der Wirksamkeit nationaler Gesetzgebung zur Vorratsspeicherung elektronischer Kommunikationsdaten beschäftigt und einer allgemeinen und unterschiedslosen VDS erneut eine deutliche Absage erteilt. Das neue Urteil schreibt die Argumente aus dem Digital-Rights-Urteil fort und stellt die den Mitgliedstaaten bei Erlass nationaler Bestimmungen unionsrechtlich auferlegten Mindestanforderungen klar.
Die europäischen Richter führen aus, dass der Grundsatz der Verhältnismäßigkeit zu beachten sei und der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene verlange, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen. Eine nationale Regelung, die eine allgemeine und unterschiedslose Vorratsdatenspeicherung vorsehe, überschreite die Grenzen des absolut Notwendigen und könne nicht als gerechtfertigt angesehen werden.

Der EuGH legt in seinem Urteil eine Reihe von Mindestanforderungen an nationale Regelungen vor. So müssten klare und präzise Regeln über die Tragweite und die Anwendung der VDS vorgesehen werden. Es müsste angegeben werden, unter welchen Umständen und unter welchen Voraussetzungen eine Maßnahme der VDS vorbeugend getroffen werden dürfe. Die Vorratsspeicherung der Daten müsse objektiven Kriterien genügen, die einen Zusammenhang zwischen den zu speichernden Daten und dem verfolgten Ziel herstellten. Der Umfang der Maßnahme und infolgedessen die betroffenen Personenkreise seien wirksam zu begrenzen.

So ist es nach der Rechtsprechung des EuGH nur zulässig, im Einzelfall eine VDS vorzunehmen, wenn ein ausreichender Anlass besteht. Hiernach dürfen nur die Personen erfasst werden, die einen Anhaltspunkt für einen Bezug zu schweren Straftaten bieten. Zudem muss die VDS auf eine Region begrenzt sein, für die der Anlass gilt. Ferner darf die VDS nur für einen bestimmten Zeitraum gelten, in dem der Anlass besteht und nur die TK-Medien betreffen, die für den Anlass relevant sind.

Diese Anforderungen erfüllen die §§ 113a – 113g TKG nicht. Das Gesetz der großen Koalition verstößt gegen die Maßstäbe des Europäischen Gerichtshofes zur VDS, indem es weiterhin eine alle Nutzer erfassende, anlasslose, flächendeckende und personell, zeitlich und geografisch undifferenzierte Speicherung aller relevanten Verkehrsdaten vorsieht.

Ferner wird das Gesetz auch zwei weiteren Anforderungen des Urteils nicht gerecht. Es ist keine Ausnahme für Kommunikationsvorgänge vorgesehen, die einem Berufsgeheimnis unterliegen, jedenfalls nicht im Zusammenhang mit den in § 53 Abs. 1 StPO genannten Berufsgeheimnisträgern. Darüber hinaus fehlt es an der Beschränkung auf die Bekämpfung schwerer Straftaten bei der Verwendung der VDS-Daten für eine Bestandsdatenauskunft zu dynamischen IP-Adressen.

Insofern ist das aktuelle Gesetz als europarechts- und verfassungswidrig anzusehen und müsste seitens der Bundesregierung bzw. seitens der Regierungsfraktionen außer Kraft gesetzt oder zumindest erheblich nachgebessert werden. Aus datenschutzrechtlicher Sicht ist es bedauerlich, dass die handelnden Akteure dies offenbar nicht planen, im Gegenteil: Der Bundesinnenminister hat sogar gefordert, die Metadatenabschöpfung bei der VDS zukünftig auch auf soziale Medien und auf Messengerdienste auszudehnen. Dieser Vorschlag missachtet auch ein Gutachten des wissenschaftlichen Dienstes des Bundestages, das ebenfalls zu dem Schluss kommt, dass die aktuelle Gesetzeslage in Deutschland nicht den Vorgaben des Europäischen Gerichtshofes entspreche.

1.2 Urteilsspruch zum BKA-Gesetz setzt Maßstäbe bei der Datenschutzaufsicht

Nicht verfassungswidrig aber unverhältnismäßig – so lautet das Urteil des Bundesverfassungsgerichts zum Bundeskriminalamtsgesetz. Damit werden neue Maßstäbe bei der Datenschutzaufsicht gesetzt; sowohl bei verdeckt durchgeführten Ermittlungen als auch bei der weiteren Verwendung der erhobenen Daten.

Das Bundesverfassungsgericht hat mit seiner Entscheidung am 20.04.2016 (1 BvR 966/09 und 1 BvR 1140/09) zum Bundeskriminalamtgesetz (BKAG) aus Sicht des Datenschutzes ein vielbeachtetes Grundsatzurteil gefällt. Zahlreiche Befugnisnormen für den Einsatz von heimlichen Überwachungsmaßnahmen, um Gefahren des internationalen Terrorismus abwehren zu können, sind zwar nicht in Gänze verfassungswidrig. Die Ausgestaltung im Einzelnen verstößt jedoch an zahlreichen Stellen gegen den Grundsatz der Verhältnismäßigkeit. Die beanstandeten Vorschriften gelten bis zum Ablauf des 30. Juni 2018 weiter. In der Zwischenzeit ist der Gesetzgeber aufgefordert, die gesetzlichen Regelungen an die Maßstäbe des Urteils anzupassen. Dies betrifft nicht nur den Bund, sondern auch die Länder. So sind zahlreiche Regelungen des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung nach dem Urteil verfassungswidrig und damit zu ändern (vgl. Seite 28).

Die Entscheidung führt eine langjährige Rechtsprechung des Bundesverfassungsgerichts systematisch zusammen. Dies betrifft sowohl die Voraussetzungen für verdeckt durchgeführte Ermittlungsmaßnahmen der Sicherheitsbehörden als auch die Frage der weiteren Verwendung der erhobenen Daten. Ferner äußert sich das Gericht ausführlich zur Datenübermittlung an andere inländische Behörden und stellt erstmals Kriterien für eine Datenübermittlung an ausländische Behörden auf. Neue Maßstäbe setzt das Bundesverfassungsgericht bei der Datenschutzaufsicht.

Aus Sicht des Datenschutzes sind folgende Erwägungen des Urteils besonders bedeutsam:

- Greifen verdeckt durchgeführte Ermittlungsmaßnahmen besonders tief in die Privatsphäre der Betroffenen (z. B. bei der Wohnraumüberwachung) ein, ist es Aufgabe des Gesetzgebers, einen angemessenen Ausgleich zwischen der Schwere des Grundrechtseingriffs und der Pflicht des Staates zum Schutz der Bevölkerung (Gefahrenabwehr und Strafverfolgung) zu schaffen. Der Verfassungsgrundsatz der Verhältnismäßigkeit verlangt, dass derartige Ermittlungsbefugnisse auf den Schutz gewichtiger Rechtsgüter begrenzt bleiben.

- Der Einsatz von besonderen Mitteln zur Überwachung außerhalb von Wohnungen erfordert grundsätzlich einen Richtervorbehalt, sofern eine Datenerhebung durch langfristige Observation stattfindet oder nichtöffentliche Gespräche erfasst werden.

- Bei der Wohnraumüberwachung oder beim Zugriff auf informationstechnische Systeme, sog. Online-Durchsuchung von Computern, sind besonders strenge Regelungen zum Schutz des Kernbereichs privater Lebensführung erforderlich. So sind nach Durchführung derartiger Maßnahmen zunächst alle erhobenen Daten von einer unabhängigen Stelle zu sichten, um höchstpersönliche Informationen auszusortieren.

- Verdeckt durchgeführte Überwachungsmaßnahmen, die typischerweise dazu führen können, in den strikt geschützten Kernbereich privater Lebensgestaltung einzudringen, bedürfen besonderer gesetzlich normierter Schutzregelungen. Erst diese flankierenden Regelungen machen die Maßnahme verhältnismäßig. Die verfassungsrechtlichen Anforderungen an Transparenz, individuellen Rechtsschutz sowie unabhängige Kontrollen müssen erfüllt sein. Hierzu gehören die Pflicht zur Benachrichtigung betroffener Personen, richterliche Kontrollbefugnisse, regelmäßige Kontrollen einer unabhängigen Aufsicht, umfassende Protokollierungspflichten, Berichtspflichten gegenüber dem Parlament und der Öffentlichkeit sowie wirksame Löschungspflichten.

- Besondere Bedeutung hat eine regelmäßige datenschutzrechtliche Kontrolle, denn diese kompensiert den bei verdeckt durchgeführten Überwachungsmaßnahmen schwach ausgeprägten Individualrechtsschutz der Bürgerinnen und Bürger. Zukünftig haben die Datenschutzaufsichtsbehörden im Zweijahresturnus die Maßnahmen zu überprüfen. Diese zusätzliche Aufgabe ist bei der Personalausstattung der Aufsichtsbehörden zu berücksichtigen, so die ausdrückliche Forderung des Bundesverfassungsgerichts.

- Nach dem Grundsatz der Zweckbindung dürfen Daten über das ursprüngliche Ermittlungsverfahren hinaus im Rahmen der festgelegten Zweckbestimmung weiter genutzt werden, solange die erhebungsberechtigte Behörde die Daten im selben Aufgabenkreis zum Schutz derselben Rechtsgüter und zur Verfolgung oder Verhütung derselben Straftaten nutzt.

- Eine zweckändernde Nutzung der Daten hat sich am Grundsatz der hypothetischen Datenneuerhebung zu orientieren. Die neue Datennutzung muss dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnte.

- Bei Daten, die aus einer Wohnraumüberwachung oder einem Zugriff auf informationstechnische Systeme stammen, gelten für eine weitere oder zweckändernde Nutzung strengere Maßstäbe. Hier müssen zusätzlich die für die Datenerhebung maßgeblichen Anforderungen an die Gefahrenlage erfüllt sein. Dies ist nur dann der Fall, wenn eine dringende oder im Einzelfall hinreichend konkretisierte Gefahrenlage vorliegt.

- Die generelle Übermittlung von Daten, die zum Zweck der Gefahrenabwehr erhoben wurden, an Strafverfolgungsbehörden ist verfassungswidrig. Daten dürfen nur zur Verfolgung solcher Straftaten genutzt werden, für die sie mit entsprechenden Mitteln erhoben werden dürften. Darüber hinaus muss ein gleichgewichtiger Rechtsgüterschutz vorliegen. Diese Grundsätze gelten auch bei der Übermittlung von Daten an Nachrichtendienste.

- Eine Übermittlung von Daten an Strafverfolgungsbehörden, die aus einer optischen Wohnraumüberwachung zum Zweck der Gefahrenabwehr stammen, ist verfassungswidrig.

- Eine Übermittlung von Daten an ausländische Sicherheitsbehörden ist zu begrenzen, da auch hier die allgemeinen Grundsätze der Zweckbindung und Zweckänderung gelten und die deutschen Sicherheitsbehörden an die Grundrechte gebunden bleiben. Bei der Entscheidung zur Datenübermittlung ist die Eigenständigkeit der anderen Rechtsordnung zu beachten. Geboten ist aber die Gewährleistung eines angemessenen datenschutzrechtlichen Niveaus im Umgang mit den übermittelten Daten im Drittstaat. Die Verletzung elementarer rechtsstaatlicher Grundsätze im Empfängerstaat schließt eine Datenübermittlung jedenfalls aus. Auch ist eine Begrenzung auf hinreichende gewichtige Zwecke, für die die Daten übermittelt und genutzt werden dürfen, vorzusehen.

- Datenübermittlungen im Inland und auch ins Ausland unterliegen zukünftig einer regelmäßigen Kontrolle durch die Datenschutzbehörden. Um diese Kontrolle effektiv ausüben zu können, sind im Gesetz Berichtspflichten für die übermittelnden Behörden zu verankern.

1.3 Gesetz über die öffentliche Sicherheit und Ordnung:

Kritik der Datenschutzbeauftragten bleibt von Landesregierung weitgehend unbeachtet

Im Berichtszeitraum hat die Landesregierung einen Gesetzentwurf zur umfassenden Novellierung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) erarbeitet und mit Beschluss vom 22.03.2016 zur Verbandsbeteiligung freigegeben. Ausgangsbasis für die Novellierung ist der Koalitionsvertrag der Regierungsfraktionen aus dem Jahr 2013, der u. a. auch eine Stärkung der Bürgerrechte und des Datenschutzes vorsieht.

In einer ersten umfassenden Stellungnahme vom 19.05.2016 hat meine Behörde eine Reihe von Änderungen datenschutzrechtlich begrüßt, wie z. B. die spezialgesetzliche Regelung der Meldeauflage, die konkrete Fassung der Befugnisnormen zur Videoüberwachung, die Streichung der Rechtsgrundlage für das sog. Kennzeichenlesegerät oder die Einschränkung der Wohnraumüberwachung. Auf der anderen Seite wurden jedoch auch zahlreiche datenschutzrechtliche Bedenken geltend gemacht. So sieht der Gesetzentwurf die Beibehaltung der sog. anlassunabhängigen Personenkontrollen nach § 12 Abs. 6 Nds. SOG ebenso vor wie die Möglichkeit einer verdeckten Videoüberwachung nach § 32 Abs. 2 Nds. SOG. Auch die neu geschaffene Ermächtigungsgrundlage für den Einsatz von Körperkameras zum Eigenschutz von Polizeivollzugsbeamten weist noch datenschutzrechtliche Mängel auf, genau wie die Rechtsgrundlage für die Veröffentlichung von personenbezogenen Daten im Internet, die sog. „Facebookfahndung".

Hingewiesen wurde auch auf die zwischenzeitlich ergangene Entscheidung des Bundesverfassungsgerichts vom 20.04.2016 zum BKA-Gesetz (siehe hierzu Seite 25). Das Innenministerium hat daraufhin einen komplett überarbeiteten Gesetzentwurf erstellt, der von der Landesregierung am 02.08.2016 beschlossen und dem Landtag zur Beratung zugeleitet wurde. Zu diesem Regierungsentwurf fand am 17.11.2016 eine öffentliche Anhörung im Ausschuss für Inneres und Sport statt.

Da zahlreiche Anregungen meines Hauses im Rahmen der Verbandsbeteiligung vom Innenministerium nicht aufgegriffen wurden, konnten diese bei der Anhörung noch einmal thematisiert werden. Wesentliche Kritikpunkte waren dabei:

- Obwohl der Koalitionsvertrag die Abschaffung bzw. Einschränkung der anlassunabhängigen Personenkontrollen nach § 12 Abs. 6 vorsieht, werden diese unverändert beibehalten. Derartige Kontrollen verstoßen gegen das Rechtsstaatsprinzip und gegen den Grundsatz der Verhältnismäßigkeit, denn es gibt keine allgemeine Pflicht des Bürgers, ohne konkreten Anlass seine Identität gegenüber der Polizei offenlegen zu müssen.

- Obwohl die Voraussetzungen für eine offene Videoüberwachung konkreter formuliert werden, hält der Gesetzentwurf weiter an der Möglichkeit einer heimlichen Videoüberwachung öffentlicher Straßen und Plätze fest. Eine für die Betroffenen nicht erkennbare Kameraüberwachung kann diese jedoch nicht davon abhalten, Straftaten zu begehen. Da das Land nur für eine präventiv wirkende Videoüberwachung die Gesetzgebungskompetenz besitzt, ist die Regelung zur heimlichen Videoüberwachung verfassungswidrig.

- Die neu geschaffene Befugnisnorm für den Einsatz sog. Bodycams muss überarbeitet werden. Insbesondere fehlen Regelungen, wer das Bildmaterial auswerten darf und wie lange dieses aufzubewahren ist.

- Der Gesetzentwurf muss zudem an zahlreichen Stellen ergänzt werden, um das in anderen Ländern übliche Datenschutzniveau zu erreichen. So fehlen insgesamt bereichsspezifische Regelungen zur Zweckänderung und Löschung von Daten, vor allem bei der Videoüberwachung. Gleiches gilt für einzelne Datenerhebungsbefugnisse, wie z. B. die Rasterfahndung. In anderen Polizeigesetzen wie z. B. Bayern, Baden-Württemberg, Berlin, Brandenburg, Bremen, Hessen oder Nordrhein-Westfalen ist das bereits heute Standard. Auch fehlen Speicherhöchstfristen für bestimmte Personengruppen wie Kontakt- und Begleitpersonen, Zeugen oder Opfer von Straftaten.

Erfreulicherweise finden sich einzelne Vorschläge meines Hauses im Gesetzentwurf wieder. Hierzu zählt eine ausdrückliche Rechtsgrundlage für die Videoüberwachung zum Zweck der Verkehrslenkung und für die sog. Abschnittskontrolle zur Überwachung der Geschwindigkeiten von Kraftfahrzeugen, auch bekannt unter dem Namen „Section Control" (vgl. Seite 39). Die weiteren Beratungen des Gesetzentwurfs im parlamentarischen Verfahren werden von meiner Behörde weiter aufmerksam verfolgt mit dem Ziel, den Datenschutz im Gefahrenabwehrrecht und bei der Strafverfolgung zu verbessern.

1.4 Novellierung des Verfassungsschutzgesetzes: Stärkung des Datenschutzes

Im Berichtszeitraum hat der Landtag am 14.09.2016 das „Gesetz zur Neuausrichtung des Verfassungsschutzes im Land Niedersachsen" in abschließender Lesung beraten. Das Gesetz ist zum 01.11.2016 in Kraft getreten. Im Zuge der fast zweijährigen Beratung durch das Parlament wurde der Entwurf der Landesregierung an zahlreichen Stellen grundlegend überarbeitet.

Das Gesetz verfolgt u. a. das Ziel, die Arbeit des Verfassungsschutzes stärker zu kontrollieren und transparenter zu gestalten. Damit soll das Vertrauen in die Arbeit des Nachrichtendienstes und des Rechtsstaates insgesamt gestärkt werden. Die Dokumentationspflichten der Verfassungsschutzbehörde bei Datenerhebungen und Datenübermittlungen an andere Behörden wurden erheblich ausgeweitet. Zusätzlich wurden Kontrollelemente auf unterschiedlichen Ebenen implementiert. Das Gesetz erweitert auch die Anordnungs- und Zustimmungsvorbehalte bei besonders eingriffsintensiven Maßnahmen sowie die Berichtspflichten gegenüber dem parlamentarischen Kontrollgremium des Landtages.

Neben neuen Regelungen zur Einstufung von Beobachtungs- und Verdachtsobjekten bzw. der Verdachtsgewinnung wurden auch die Vorschriften zur Datenverarbeitung grundlegend überarbeitet und im „Dritten Teil" des Gesetzes zusammengefasst. Zukünftig werden in engerer Anlehnung an datenschutzrechtliche Grundprinzipien die einzelnen Phasen der Datenverarbeitung und damit die gesetzlichen Voraussetzungen für die Erhebung, Speicherung, Übermittlung von Daten näher geregelt.

Unter dem Eindruck der mutmaßlich islamistisch motivierten Messerattacke einer 15-Jährigen auf einen Bundespolizisten in Hannover erlaubt die finale Fassung des Gesetzes anders als ursprünglich geplant, auch weiterhin die Beobachtung von 14- und 15-jährigen Jugendlichen. Dabei gelten für die Erhebung sowie für die Speicherung der Daten der Minderjährigen jedoch strengere Voraussetzungen als bisher.

Zu begrüßen ist es, dass mit dem neuen Verfassungsschutzgesetz die Vorgaben der Rechtsprechung des Bundesverfassungsgerichtes (u. a. Urteil vom 20.04.2016 zum BKA-Gesetz, S. 25 TB) berücksichtigt werden.

Dies betrifft insbesondere die Regelungen zur Datenübermittlung zwischen Polizei und Verfassungsschutz (§§ 31 und 32 NVerfSchG) sowie auf die verschärften Anforderungen zum Schutz von Daten, die den Kernbereich privater Lebensgestaltung betreffen (§ 10 NVerfSchG). Ferner sieht § 39 Abs. 2 NVerfSchG vor, dass meine Behörde zukünftig im Abstand von höchstens

zwei Jahren regelmäßig die Einhaltung der gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten zu überprüfen hat, die mit nachrichtendienstlichen Mitteln erhoben wurden. Dies betrifft insbesondere Daten, die der Verfassungsschutz mit heimlichen Maßnahmen und damit ohne Kenntnis der betroffenen Personen erhebt, also z. B. im Rahmen einer verdeckt durchgeführten Observation.

Verfassungsschutzgesetz stärkt Kontrollbefugnisse der Landesbeauftragten für den Datenschutz

Ferner sieht das Gesetz in § 39 Abs. 1 vor, dass der Ausschuss für Angelegenheiten des Verfassungsschutzes meine Behörde beauftragen kann, die Rechtmäßigkeit einzelner Maßnahmen zu überprüfen. Das dafür erforderliche Quorum wurde von einem Viertel auf ein Fünftel der Abgeordneten gesenkt. Die Kontrollbefugnisse meiner Behörde zur Einhaltung des Datenschutzes beim Verfassungsschutz wurden mithin auch an dieser Stelle weiter gestärkt.

1.5 Telekommunikationsüberwachung: Anlage in Niedersachsen und Bremen weiterhin rechtswidrig

In meinen Tätigkeitsberichten für die Jahre 2011 und 2012 bzw. für die Jahre 2013 und 2014 habe ich umfassend über erhebliche datenschutzrechtliche Mängel beim technisch-organisatorischen Datenschutz bei der polizeilichen Telekommunikationsüberwachung (TKÜ) berichtet. Diese Mängel sind Ende 2016 immer noch vorhanden.

Aufgrund der datenschutzrechtlichen und technisch-organisatorischen Bewertung des Schutzbedarfes, der erheblichen Eingriffstiefe in Grundrechte und der allgemein erheblichen Risiken bei der TKÜ für die informationelle Selbstbestimmung der Betroffenen sehe ich weiterhin eine immense Bedeutung darin, vollständige und angemessene Schutzmaßnahmen für das seit Oktober 2012 laufende Verfahren umzusetzen. Die seit 2012 ausstehende Mängelbeseitigung wurde im Berichtszeitraum weiterhin eingefordert. Dies geschah zum einen in eigener Landeszuständigkeit, aber ebenso auch in Abstimmung mit der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen (LfDI Bremen), weil im LKA Niedersachsen auch für die Polizei des Bundeslandes Bremen die technische Dienstleistung erbracht wird.

Erhebliche Defizite

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

- 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 partiellen Datenlöschung im Kernbereich privater Lebensgestaltung[1] sowie zur Mandantentrennung für verschiedene Polizeibehörden und -dienststellen.

Umfassender Mängelkatalog

In einem vorläufigen Zwischenergebnis nach intensiver Prüfung der vorliegenden Unterlagen wurde eine Reihe von Datenschutzmängeln festgestellt. Zum Zeitpunkt der mit der LfDI Bremen gemeinsam durchgeführten Prüfung befand sich die TKÜ-Anlage bereits seit Oktober 2012 im Wirkbetrieb. Das Niedersächsische Ministerium für Inneres und Sport (MI) wurde erstmals im August 2013 über die bestehenden Mängel informiert. Im September 2013 fand zwischen meinem Amtsvorgänger und dem Innenminister ein Gespräch statt, in dem die Kernpunkte der Mängel deutlich gemacht wurden. Deren intensive Bearbeitung und Beseitigung sollte auf Seiten des LKA nunmehr mit hoher Priorität vorangetrieben werden. Über weitere Maßnahmen sollte meine Behörde informiert werden. Da auf Seiten meiner Behörde der dazu erforderliche hohe Sach- und Zeitaufwand bekannt war, war mit einer Lösung nicht kurzfristig in den Folgemonaten zu rechnen. Mit Beginn meiner Amtszeit drängte ich jedoch auf Lösungen. Nachdem seitens des LKA und des MI keine Mitteilungen über erwartete Fortschritte erfolgten, kam es am 11.06.2015 zu neuen fachlichen Gesprächen zwischen meiner Behörde und Vertretern des LKA bzw. des MI über den Sachstand der datenschutzrechtlichen und technisch-organisatorischen Fragen des Verfahrens. Es wurde deutlich, dass diese Gespräche fortgesetzt werden mussten. Ein letztes Gespräch fand am 29.06.2016 statt. Im Ergebnis bleibt jedoch festzuhalten, dass eine den Datenschutz wesentlich verbessernde Mängelbeseitigung im Berichtszeitraum nicht stattgefunden hat. Dies zeigt auch die Antwort der Landesregierung auf eine mündliche Anfrage von drei Abgeordneten der FDP-Fraktion.[2] Dort sind folgende sieben gebündelte Problemfelder als noch offen aufgelistet:

1. Die Aussagen zur Risikoanalyse sind weiterhin unvollständig.
2. Die erforderliche Mandantenfähigkeit des Verfahrens im datenschutzrechtlichen Sinn ist nicht erwiesen.
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 kann.
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.

1 Der Kernbereichsschutz gem. § 100a Abs. 4 Strafprozessordnung (StPO) fußt auf der vom Bundesverfassungsgericht in mehreren Entscheidungen geforderten Differenzierung zwischen Daten, die unter normenklaren Bedingungen ermittelt und verarbeitet werden dürfen, und Daten, die dem unantastbaren Kernbereich privater Lebensumstände zuzuordnen sind. Letztere unterliegen dem absoluten, also ausnahmslosen Schutz vor staatlichen Eingriffen, dürfen folglich nicht erhoben werden und unterliegen einem Beweisverwertungsverbot. Werden sie im Zuge eines mitgeschnittenen Datenstreams oder eines Telefonates dennoch unvermeidbar erhoben, sind sie unverzüglich nach Identifizierung als solche rückstandsfrei zu löschen. Vgl. zuletzt BVerfGE 141, 220-378 m. w. N.

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

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

Festzuhalten bleibt, dass es dem LKA Niedersachsen als verantwortlicher Stelle und dem MI als Fachaufsichtsbehörde trotz zahlreicher Gespräche und Ankündigungen bis zum Ende des Berichtszeitraums nicht gelungen ist, die umfangreiche Mängelliste maßgeblich abzuarbeiten. Von den insgesamt 44 festgestellten Mängeln[3] werden sich nach der Kündigung des Dienstleisters nur wenige beseitigen lassen. Die besonders schwer wiegenden Mängel bei der Mandantentrennung, der unzureichenden Protokollierung und der mangelhaften Verschlüsselung der Inhalts- und Verkehrsdaten führen dazu, dass der Betrieb der TKÜ-Anlage nach wie vor aus Sicht des Datenschutzes rechtswidrig ist.

Ungewisse Zukunft für RDZ der Küstenländer

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 den Tätigkeitsberichten für die Jahre 2011/2012 und 2013/2014 ausführlich geäußert. Die beteiligten Länder Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein wollen auf der Grundlage eines Staatsvertrages gemeinsam eine Anlage zur Telekommunikationsüberwachung errichten und betreiben, die mittelfristig die bestehenden und technisch überholten TKÜ-Anlagen ersetzen soll. Dies betrifft auch die laufende TKÜ-Anlage beim LKA Niedersachsen, die Telekommunikationsvorgänge zur Strafverfolgung und Gefahrenabwehr für niedersächsische und bremische Behörden überwachen kann.

Auch im Berichtszeitraum wurde das Thema „RDZ-TKÜ" wiederholt auf Fachebene der Rechts- und Technikreferate der Datenschutzbeauftragten der beteiligten Bundesländer erörtert, insbesondere vor dem Hintergrund der Erfahrungen mit dem Wirkbetrieb der laufenden Anlage beim LKA Niedersachsen und der dort festgestellten erheblichen datenschutzrechtlichen Mängel. Es besteht Einigkeit mit den vier anderen Landesdatenschutzbeauftragten, dass Erfahrungen mit dem Hersteller und Dienstleister der TKÜ-Software für die TKÜ-Anlage beim LKA Niedersachsen bezüglich nicht geleisteter oder leistbarer Anpassungen an datenschutzrechtliche Anforderungen auch erhebliche Auswirkungen auf künftige Ausschreibungen und Leistungsbeschreibungen im Rahmen des Projekts „RDZ-TKÜ" haben müssen; dies umso mehr, als grundlegende Mängel oder Schwachstellen eine flächendeckende Wirkung auf Betroffene in fünf Bundesländern haben würden.

Stand des Projekts

Im Berichtszeitraum wurde der zwischen den fünf norddeutschen Ländern unterzeichnete Staatsvertrag durch entsprechende Landesgesetze ratifiziert. In Niedersachsen hat die Landesregie-

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

rung im April 2016 dem Landtag einen entsprechenden Gesetzentwurf[4] zugeleitet, zu dem ich anlässlich der Beratung im Ausschuss für Inneres und Sport am 19.05.2016 angehört wurde. Grundlage meiner Ausführungen war eine gemeinsame Stellungnahme der Datenschutzbehörden der fünf beteiligten Länder. In dieser wird die Einrichtung eines gemeinsamen Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung auf der Grundlage eines Staatsvertrages ausdrücklich begrüßt. Jedoch weisen die Aufsichtsbehörden auch darauf hin, dass bei einer Telekommunikationsüberwachung höchst sensible personenbezogene Daten erhoben und verarbeitet werden, beispielsweise auch Daten, die den Kernbereich der privaten Lebensgestaltung betreffen. Daher spielen bei dem Projekt RDZ-TKÜ der Datenschutz und die Datensicherheit eine überragende Rolle. Im Ergebnis kann konstatiert werden, dass der Staatsvertrag diesen Anforderungen genügt. Änderungswünsche der Datenschutzbehörden wurden in den Staatsvertrag übernommen, so z. B. eine ausdrückliche Regelung zur Aufsicht über das RDZ, um datenschutzrechtliche Mängel, die bei einer Prüfung durch eine Aufsichtsbehörde festgestellt werden, wirksam beseitigen zu können. Auch stellt der Staatsvertrag sicher, dass die Datenschutzbehörden bei allen Fragen und Entscheidungen zum Datenschutz und zur Datensicherheit eng eingebunden werden.

Ferner fand im Mai 2016 eine Besprechung der fünf Datenschutzbehörden in beratender Funktion mit dem LKA Niedersachsen als projektverantwortlicher Stelle statt. Auf Bitte des LKA Niedersachsen zur Vorbereitung des Vergabeverfahrens für den Dienstleister und die Systemtechnik ging es um die Frage, welche datenschutzrechtlichen Anforderungen an eine Datenverarbeitung im Auftrag bei Maßnahmen der Telekommunikationsüberwachung zu stellen sind. Die Datenschutzbehörden empfehlen u. a., den Zugriff des Dienstleisters in seiner Funktion als Auftragsdatenverarbeiter 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.

Eine weitere Meldung des LKA oder MI über Fortschritte zur Lösung der bestehenden Mängel ist trotz meiner eindeutigen Hinweise, dass der Status nicht hinnehmbar ist, im letzten Zeitabschnitt des Berichtszeitraumes nicht erfolgt. Das LKA bezieht sich unterdessen auf die faktischen Hemmnisse aufgrund der Produktabkündigung durch den Dienstleister und zum anderen auf die zu erwartende Neuprojektierung gemeinsam mit den fünf norddeutschen Ländern, die grundlegende Verbesserungen mit sich bringen könnten.
Ich werde die Projektierung ab 2017 – gemeinsam mit den anderen Aufsichtsbehörden – von Beginn an beobachten, um auf die Vermeidung derartiger Mängel in dem neuen Verfahren durch intensive Beratung hinzuwirken.

Rechtsgrundlagen:
Nach dem Telekommunikationsgesetz (TKG) und der Strafprozessordnung (StPO) sieht der Gesetzgeber bei bestimmten schweren Straftaten vor, dass die Ermittlungsbehörden die Telekommunikation von Personen überwachen (Telekommunikationsüberwachung – TKÜ) und die Telekommunikationsanbieter dabei mitwirken. Das Gefahrenabwehrrecht enthält durch das TKG und das Niedersächsische Gefahrenabwehrgesetz ebenfalls Rechtsnormen, die die TKÜ erlaubt.

4 LT-Drs. 17/5619

1.6 Rechtswidriger Einsatz von Bodycams durch die Polizei

Seit Jahren wird der Einsatz sog. Bodycams durch die Polizei zum Schutz der Polizeibeamten vor gewalttätigen Übergriffen diskutiert. Als erstes Bundesland hat Hessen im Jahr 2015 sein Polizeirecht geändert, um dieses neue Einsatzmittel auf eine gesicherte rechtliche Grundlage zu stellen. Andere Länder wie z. B. Hamburg, Bremen, Baden-Württemberg und Nordrhein-Westfalen sind diesem Beispiel gefolgt. Es ist zu erwarten, dass in naher Zukunft alle Polizeibehörden in Deutschland Bodycams einsetzen werden.

Der am 02.08.2016 von der Landesregierung beschlossene Gesetzentwurf zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) sieht u. a. auch eine neue und damit ausdrückliche Rechtsgrundlage für die Nutzung von Bodycams durch die Polizei vor (siehe § 32 Abs. 4 Satz 2 neu).[1] Hierzu fand im Ausschuss für Inneres und Sport am 17.11.2016 eine umfassende Sachverständigenanhörung statt, bei der sich alle Beteiligten einig waren, dass der Einsatz von Bodycams vom Gesetzgeber im Einzelnen zu regeln ist. Hinsichtlich der von der Landesregierung vorgeschlagenen neuen Befugnisnorm des § 32 Abs. 4 Satz 2 sahen alle Sachverständigen noch erheblichen Erörterungsbedarf.

Landesweites Pilotverfahren auf mangelhafter Rechtsgrundlage

Obwohl das Parlament noch nicht abschließend über den Einsatz von Bodycams beraten hatte, verkündete der Innenminister am 12.12.2016 im Rahmen einer Pressekonferenz den Start eines Pilotprojekts zur landesweiten Erprobung von Bodycams bei der Polizei. Beschafft wurden 20 Körperkameras, die von den Beamtinnen und Beamten in den verschiedensten Einsatzbereichen eingesetzt werden sollten, so z. B. auf Weihnachtsmärkten oder bei Personenkontrollen. Es sollten nur Bildaufzeichnungen angefertigt werden, nicht jedoch Tonaufnahmen. Eine neue Rechtsgrundlage sei hierfür nicht erforderlich, da der Pilotversuch auf § 32 Abs. 4 Satz 1 Nds. SOG gestützt werde.

Diese Kehrtwendung kam nicht nur für die Abgeordneten, sondern auch für meine Behörde völlig unerwartet. Noch Ende November, anlässlich der Innenministerkonferenz, vertrat der Innenminister die Rechtsansicht, dass für den Einsatz von Bodycams zunächst das Polizeigesetz geändert werden müsse.[2]

1 LT-Drs. 17/6232, vgl. hierzu auch S. 28

2 205. Sitzung der Innenministerkonferenz, 29.11. bis 30.11.2016 in Saarbrücken, TOP 6 (Auswertung der Pilotprojekte zum Einsatz von Body-Cams)

Dies ist aus folgenden Gründen auch meine Rechtsauffassung:

Die personenbezogene Videoüberwachung mittels einer Körperkamera (Bodycam) greift in das Grundrecht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und in das Grundrecht auf allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG der Betroffenen ein. Da die Kamera auf Schulterhöhe getragen direkt in das Gesicht der betroffenen Personen filmt, wird auch in das Recht am eigenen Bild (§ 22 Satz 1 Kunsturhebergesetz i. V. m. Art. 1 Abs. 1 GG) eingegriffen. Direkte Gesichtsaufnahmen der Zielperson, die durch ihr Fehlverhalten den Kameraeinsatz ausgelöst hat, aber auch mögliche Porträtaufnahmen völlig unbeteiligter Personen führen dazu, dass die Grundrechtseingriffe als besonders schwerwiegend einzustufen sind.

Für den Einsatz von Bodycams durch die Polizei ist demzufolge zur Rechtfertigung der schwerwiegenden und spezifischen Grundrechtseingriffe eine spezielle Befugnisnorm im Nds. SOG erforderlich, die eindeutig und damit dem Bestimmtheitsgrundsatz genügend definiert, in welchen Situationen und zu welchen Zwecken personenbezogene Daten erhoben und verarbeitet werden dürfen. Dies gilt ebenso für den laufenden Pilotbetrieb, der den Kameraeinsatz im Arbeitsalltag der Polizei erproben soll. Auch im Pilotbetrieb werden Echtdaten der betroffenen Personen erhoben und verarbeitet.

Einsatz von Bodycams erfordert neues Recht

Diesen Anforderungen genügt die vorhandene Rechtsgrundlage des § 32 Abs. 4 Satz 1 Nds. SOG nicht. Nur scheinbar erfasst der Wortlaut dieser Norm, die Ende 2003 ins Nds. SOG eingefügt

wurde, auch den Einsatz von Körperkameras. Jedoch gab es zu dieser Zeit noch keine bewegliche Kameratechnik, die am Körper des Beamten getragen werden konnte, so dass der Gesetzgeber diese spezielle Form der Videoaufzeichnung als Regelungsgegenstand nicht im Blick haben konnte. Vielmehr hat der Gesetzgeber seinerzeit nur fest im Streifenwagen installierte Kameras als besondere Form der Videoüberwachung regeln wollen.

Ein Blick in die Polizeigesetze anderer Länder bestätigt diese Rechtsauffassung. So fügte beispielsweise Hamburg 2005 eine dem § 32 Abs. 4 Satz 1 entsprechende Regelung in das Gesetz über die Datenverarbeitung in der Polizei ein.[3] Dennoch sah sich der Hamburger Senat genötigt, für den Einsatz von Bodycams im Jahr 2015 eine ausdrückliche Rechtsgrundlage zu schaffen.[4] Dies ist auch deshalb erforderlich, weil Bodycams kleine, tragbare und damit mobile Videoüberwachungseinheiten darstellen, die gerade nicht auf bestimmte Örtlichkeiten beschränkt sind wie z. B. ortsfeste Videokameras an Kriminalitätsschwerpunkten oder im Fahrzeug fest installierte Kameras, die nur bei stehendem Fahrzeug eingeschaltet werden dürfen (Anhalte- und Kontrollsituation). Auch hat die Kameratechnik einen Quantensprung vollzogen, weg von der analogen hin zur digitalen Technik mit ihren vielfältigen Auswertungsmöglichkeiten. Im Ergebnis stellen Bodycams im Vergleich zu bisherigen Formen der Videoüberwachung ein völlig anderes Einsatzmittel dar, über dessen Einsatz einzig und allein der Gesetzgeber zu befinden hat. Dies gilt insbesondere für die Frage, zu welchem Zeitpunkt die Bodycam eingeschaltet werden darf. Hierzu fehlt eine konkrete Regelung im § 32 Abs. 4 Satz 1 Nds. SOG.
Im Ergebnis habe ich das Pilotverfahren zum Einsatz von sogenannten Bodycams durch die niedersächsische Polizei wegen einer fehlenden Rechtsgrundlage kurz nach dessen Start förmlich nach § 23 Abs. 1 NDSG als rechtswidrig beanstandet. Die Beanstandung wurde auch ausgesprochen, weil die nach § 7 Abs. 3 NDSG erforderliche Vorabkontrolle vor Beginn des Pilotverfahrens vom Ministerium für Inneres und Sport nicht vorgelegt werden konnte. Diese dient der Prüfung, ob die mit der Datenverarbeitung verbundenen Risiken für die Betroffenen durch technische und organisatorische Maßnahmen wirksam beherrscht werden können.

Zum Ende des Berichtszeitraums war das bis Ende März 2017 laufende Pilotverfahren noch nicht abgeschlossen. Im nächsten Tätigkeitsbericht werde ich auf die Ergebnisse der Erprobung von Bodycams durch die Polizei näher eingehen. Gleiches gilt für die Beschaffung und den Einsatz von 500 Bodycams im November 2017.

3 § 8 Abs. 5 PolEDVG: „Die Polizei darf bei Anhalte- und Kontrollsituationen im öffentlichen Verkehrsraum durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen Daten erheben, wenn dies zum Schutz der Vollzugsbediensteten oder eines Dritten erforderlich ist."

4 GVBl. Hamburg 2015, S. 21

1.7 „Section Control“: Rechtsgrundlage für dauerhaften Betrieb zwingend notwendig

Für den geplanten dauerhaften Einsatz einer Streckengeschwindigkeitsüberwachung fehlt weiterhin die Verabschiedung einer Rechtsgrundlage durch die Landesregierung. Immerhin wurden festgestellte Mängel der Anlage beim technisch-organisatorischen Datenschutz aufgrund meiner Hinweise teilweise behoben. Verbliebene Schwachstellen sollen beseitigt und der Datenschutz weiter optimiert werden.

Das Niedersächsische Ministerium für Inneres und Sport erprobt eine Anlage zur Streckengeschwindigkeitsüberwachung (Section Control), die im Laufe des Jahres 2015 an der Bundesstraße 6 zwischen Gleidingen und Rethen auf drei Kilometern Länge errichtet wurde. Vergleichbare Anlagen gibt es beispielsweise in Österreich, der Schweiz und in den Niederlanden. Dabei werden von Fahrzeugen, deren Durchschnittsgeschwindigkeit innerhalb des festgelegten Streckenabschnitts höher ist als die zulässige Höchstgeschwindigkeit, so genannte Vorfallsdatensätze mittels des bekannten „Blitzens“ und der damit verbundenen Lichtbildaufnahme des Fahrzeugs einschließlich des Fahrzeugführers generiert, um anschließend die begangene Ordnungswidrigkeit zu ahnden.

Nach Herstellerangaben wird die Geschwindigkeitsdurchschnittsübertretung in einer Reihe von Teilschritten festgestellt: Die Fahrzeuge werden am Ein- und Ausfahrtsquerschnitt der Anlage detektiert, klassifiziert und durch Kameras fotografisch von hinten erfasst. Innerhalb der besonders gesicherten Rechnerkomponenten der Anlage sollen die Heckaufnahmen bereits am Einfahrtsquerschnitt (1. Kamera) hochverschlüsselt werden. Es wird ein sog. Hashwert generiert, der eine manuelle Rückführbarkeit auf das amtliche Kennzeichen des Fahrzeugs ausschließt. Nach dem Durchfahren 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. Im Fall der Übertretung wird anschließend der Vorfallsdatensatz durch das Auslösen des „Blitzens“ (3. Kamera) generiert. In allen anderen Fällen soll eine sofortige und unwiderrufliche Löschung der Datensätze erfolgen.

Rechtslage

Für den dauerhaften Betrieb einer Section-Control-Anlage ist nach der Rechtsprechung des Bundesverfassungsgerichts zwingend eine gesetzliche Rechtsgrundlage erforderlich. Zwar hat das Bundesverfassungsgericht in seinem Urteil vom 11.03.2008 (1 BvR 2074/05 und 1 BvR 1254/07) zum Einsatz von Kennzeichenlesesystemen in Hessen und Schleswig-Holstein einen Eingriff in

das Recht auf informationelle Selbstbestimmung nicht als gegeben angesehen, wenn das amtliche Kennzeichen unverzüglich mit dem Fahndungsbestand der Polizei abgeglichen und ohne weitere Auswertung sofort wieder gelöscht wird. In diesem sog. „Nichttrefferfall" liege gar keine Datenerhebung und damit auch kein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor. Jedoch hat das Gericht im selben Urteil auch ausgeführt, dass bei einem Trefferfall eine Datenerhebung und anschließende Datenverarbeitung stattfindet. Für diese Fälle ist daher eine Rechtsgrundlage erforderlich. Im Fall von Section Control betrifft dies alle Fahrzeuge, bei denen eine Geschwindigkeitsübertretung stattfindet.

Gleichwohl hat mein Vorgänger im Amt entschieden, die Erprobung einer Section-Control-Anlage für die Dauer von 18 Monaten zuzulassen, wenn:

- die Anlage nur zur Feststellung einer etwaigen Geschwindigkeitsübertretung genutzt wird und die erhobenen Daten somit zu keinem anderen Zweck genutzt werden,
- die Feststellung der Geschwindigkeitsübertretung oder der Nicht-Übertretung unverzüglich erfolgt,
- technisch gesichert ist, dass Nichttrefferfälle sofort spurenlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden,
- die Anlage nach ihrer Installation in einem Zeitraum von maximal 18 Monaten betrieben wird und
- durch eine eindeutige Beschilderung auf den Umstand der Überwachung hingewiesen wird.

Diese Grundsätze sind für das Pilotverfahren zwingend zu beachten.

Aktueller Stand:

Im Berichtszeitraum hat die verantwortliche Stelle, die Polizeidirektion Hannover, für das Projekt „Section Control" eine Vorabkontrolle und Verfahrensbeschreibung erstellt und meiner Behörde übersandt. Eine Gefährdungsanalyse wurde ebenfalls angefertigt. Diese dient dazu, den unberechtigten Zugriff auf personenbezogene Daten weitgehend auszuschließen und einen Missbrauch der erhobenen Daten zu verhindern. Sämtliche Unterlagen wurden von meiner Behörde eingehend datenschutzrechtlich überprüft. Zudem gab es Ende 2015 mehrere Besprechungen mit der Polizei und dem Hersteller der Section-Control-Anlage. Festgestellte Mängel der Anlage beim technisch-organisatorischen Datenschutz sind aufgrund meiner Hinweise teilweise behoben worden. Die verantwortliche Stelle bzw. der Hersteller haben zugesagt, die verbliebenen Mängel zeitnah zu beseitigen. Unter anderem soll die vom Hersteller eingesetzte Technik zur Verschlüsselung der Daten optimiert werden. Eine abschließende nochmalige Prüfung des technisch-organisatorischen Datenschutzes werde ich spätestens nach Beendigung des Pilotverfahrens vornehmen.

Letztlich hat meine Behörde im Mai 2016 der Polizeidirektion Hannover mitgeteilt, dass die getroffenen bzw. zugesagten technisch-organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten einen Pilotbetrieb für die Dauer von 18 Monaten aus datenschutzrechtlicher Sicht zulassen. Gleichzeitig habe ich darauf hingewiesen, dass für einen Echtbetrieb nach Ende der Pilotphase zwingend eine Rechtsgrundlage zu schaffen ist. Der Gesetzentwurf der Landesregierung zur Änderung des Nds. Gesetzes über die öffentliche Sicherheit und Ordnung (s. Seite 28) setzt diese Forderung um und sieht eine Ergänzung des § 32 vor, die den Betrieb einer Section-Control-Anlage und die damit verbundene Datenerhebung und -verarbeitung ausdrücklich regelt.

1.8 Datenverarbeitung der Polizei bei Teilnahme an einer friedlichen Versammlung

Ein Petent machte im Jahr 2015 eine Eingabe hinsichtlich der Verarbeitung seiner personenbezogenen Daten im Zusammenhang mit der Anmeldung bzw. der Teilnahme an einer störungsfrei verlaufenen Versammlung. Aus diesem Grund habe ich die Polizei um eine entsprechende Selektion im Vorgangsbearbeitungssystem NIVADIS gebeten.

Die Selektion erfolgte unter Einbeziehung folgender Kriterien für den Zeitraum 01.01.2003 bis 21.07.2015:

- Vorgangsart „Sonstiges Ereignis“,
- Anlass „friedliche demonstrative Aktion, Umzug, Versammlung, Aufzug“,
- Rolle der Person „Ansprechpartner, Anmelder, Verantwortlicher“.

In einem weiteren Schritt wurden lediglich solche Datensätze als relevant herausgefiltert, bei welchen noch ein Personenbezug zum Ansprechpartner, Anmelder bzw. Verantwortlichen, etwa in Form des Nachnamens, hergestellt werden konnte. Diese Ergebnismenge wurde in einem letzten Schritt wiederum um jene Ereignisse reduziert, welche eine Verknüpfung zu den Vorgangsarten „Straftat“ bzw. „Ordnungswidrigkeit“ aufweisen konnten, da in diesen Fällen in der Regel nicht von einer störungsfrei verlaufenen Versammlung ausgegangen werden kann. Abschließend erfolgte eine manuelle Sichtung der verbliebenen Datensätze hinsichtlich der Klassifizierung der Versammlung als friedlich.
Die jeweils (für die Verarbeitung der personenbezogenen Daten) verantwortlichen Polizeidirektionen wurden um Prüfung der beigefügten Vorgangsnummer insbesondere unter dem Aspekt der Erforderlichkeit der weiteren Verarbeitung in den „Sonstigen Ereignissen“ gebeten und um einen abschließenden Rücklauf bis zum Ende des 1. Quartals 2016 aufgefordert. Im Einzelnen haben die Polizeidirektionen wie folgt reagiert:

Mehrheit der Polizeidirektionen löscht personenbezogene Daten nach friedlichem Veranstaltungsverlauf

Der Polizeidirektion Hannover wurden insgesamt 66 Vorgangsnummern mit den o. g. Kriterien übermittelt. In dem Antwortschreiben teilte die Polizeidirektion Hannover mit, dass aus allen aufgeführten Vorgängen die personenbezogenen Daten gelöscht wurden, da eine Erforderlichkeit zur Speicherung der Daten nicht weiter vorlag.

Der Polizeidirektion Osnabrück wurden 45 Vorgangsnummern übermittelt. Dem Antwortschreiben konnte entnommen werden, dass aus allen betroffenen Datensätzen jeglicher Personenbezug gelöscht wurde.

Der Polizeidirektion Braunschweig wurden 106 Vorgangsnummern übermittelt. Laut Stellungnahme wurden die übermittelten Datensätze näher aufgeschlüsselt und analysiert. So stellte sich heraus, dass 29 Datensätze im Zusammenhang mit Traditionsveranstaltungen (z. B. Schützen- und Volksfeste) gespeichert waren. Die übrigen Datensätze betrafen versammlungsrechtliche Aktionen. Im Ergebnis wurden auch hier sämtliche personenbezogenen Inhalte nach eingehender Überprüfung gelöscht.

Die Polizeidirektion Oldenburg erhielt insgesamt 89 Vorgangsnummern. Auch hier wurden alle Datensätze intensiv überprüft. Nur in einem Vorgang wurde eine weitere Speicherung für erforderlich gehalten. Es handelt sich dabei um den Vorgang des Staatsschutzes in Oldenburg anlässlich einer Demonstration gegen das „Gutscheinsystem" im Asylverfahren am Rande eines Besuchs des Innenministers. Gespeichert wurde eine als linksmotivierter Straftäter bekannte Person, die bereits seit 1999 in der linken Szene durch Verstöße gegen das Versammlungsgesetz, Hausfriedensbruch, Sachbeschädigung und Körperverletzung sowie weiterer Delikte auffällig geworden ist. Alle personenbezogenen Inhalte in den übrigen Datensätzen wurden gelöscht.

Die Polizeidirektion Göttingen hatte insgesamt 71 übersandte Vorgangsnummern zu überprüfen. Aus der Stellungnahme ergibt sich, dass die personenbezogenen Daten von Anzeigenden, Durchführenden und auch Teilnehmern von Versammlungen im polizeilichen Vorgangsbearbeitungssystem NIVADIS gespeichert und die Löschfristen aus § 10 Niedersächsisches Versammlungsgesetz nicht eingehalten wurden. Auch hier wurden im Ergebnis alle personenbezogenen Angaben aus den Datensätzen (nach nochmaliger Überprüfung) gelöscht.

Die Polizeidirektion Lüneburg, der 135 Vorgangsnummern übermittelt wurden, hat mir mitgeteilt, dass sie in sieben Fällen eine Löschung der Datensätze vorgenommen habe, in 18 weiteren Fällen erfolgte nach der Überprüfung die sofortige Anonymisierung der personenbezogenen Daten, so dass eine personenbezogene Verarbeitung nur noch unter sehr engen Voraussetzungen möglich ist.
Grundsätzlich halte man jedoch an der weiteren Verarbeitung personenbezogener Daten im Vorgangsbearbeitungssystem NIVADIS fest, auch wenn die Versammlung friedlich verlaufen sei und sich keine weiteren Ermittlungen anschlössen. Als Rechtsgrundlage für die Verarbeitung bezieht sich die Polizeidirektion Lüneburg auf die Dokumentationsverpflichtung des behördlichen Handelns und sieht aus diesem Grund keine Veranlassung für eine Löschung.

Datenspeicherung aufgrund fragwürdiger Rechtsauslegung

Generell scheint sich in den Polizeidirektionen mit Ausnahme der Polizeidirektion Lüneburg die Auffassung durchzusetzen, dass personenbezogene Daten von Versammlungsleitern und -teilnehmern, die in der Form eines „Sonstigen Ereignisses" erfasst wurden und nur den Verlauf einer friedlichen Versammlung beinhalten, zu löschen bzw. erst gar nicht zu erheben sind. Dieses Vorgehen wird von mir ausdrücklich begrüßt, da es der Gesetzeslage entspricht.

Nach meiner Auffassung ist die Speicherung personenbezogener Daten von Versammlungsteilnehmern im polizeilichen Vorgangsbearbeitungssystem NIVADIS über das Versammlungsende hinaus rechtswidrig, wenn die Versammlung friedlich verlaufen ist. Dies ergibt sich aus § 10 Abs. 1 Satz 4 NVersG. Danach sind die nach § 10 Abs. 1 Satz 1 NVersG erhobenen Daten unverzüglich nach Beendigung der Versammlung unter freiem Himmel zu löschen, soweit sie nicht zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt werden. Nach meinem Verständnis gilt diese Löschungsvorschrift für alle Daten, die im Rahmen von Versammlungen erhoben wurden (Versammlungsleiter, Ordner und Teilnehmer).

Vor der Speicherung bzw. Löschung von Daten stellt sich die Frage, auf welcher Rechtsgrundlage die Polizei personenbezogene Daten von friedlichen Versammlungsteilnehmern überhaupt erhebt. Das Ministerium für Inneres und Sport wurde dazu von mir angeschrieben. Auch eine kleine Anfrage des Abgeordneten Oetjen (FDP-Fraktion) hat die Frage der Rechtmäßigkeit der Datenerhebung aufgeworfen.[1] Im Ergebnis wird die Auffassung vertreten, dass eine Datenerhebung auch nach dem Gefahrenabwehrrecht möglich sei (§ 38 Abs. 1 Satz 2 Nds. SOG) und die Frage der Datenerhebung und –speicherung immer im Einzelfall beantwortet werden müsse. Ferner gehöre zur Aufgabenerfüllung der Polizei auch die Vorgangsverwaltung zum Zweck der Verfolgung repressiver und präventiver Aufgabenstellungen. Somit sei eine Erhebung und Speicherung auch unter diesem Gesichtspunkt möglich.

Dieser Ansicht ist zu entgegnen, dass bei Datenerhebungen im Zusammenhang mit Versammlungen nicht nur in das Grundrecht auf informationelle Selbstbestimmung eingegriffen wird, sondern auch in das Grundrecht auf Versammlungsfreiheit nach Art. 8 GG. Die Polizei ist daher gehalten, besonders sensibel mit Daten von Versammlungsteilnehmern umzugehen. Jedenfalls setzt eine Datenerhebung nach dem Nds. SOG grundsätzlich voraus, dass eine Gefahrenlage besteht oder der Verdacht einer Straftat. Dies ist jedoch nicht anzunehmen, wenn eine Versammlung völlig störungsfrei verläuft und dies polizeilich auch noch dokumentiert wird. Folgendes Beispiel aus dem Datenbestand der PD Lüneburg, die gestützt von der Ansicht des Ministeriums für Inneres und Sport die Löschung des Datensatzes bisher verweigert, möge das verdeutlichen:

> Laut Kurzsachverhalt, dokumentiert im polizeilichen Vorgangsbearbeitungssystem, begleitete die Polizei eine genehmigte Versammlung des Netzwerkes XY gegen Rechtsextemismus. „Im Rahmen der Begleitung gab es keine Vorkommnisse. An den einzelnen Kundgebungsorten waren ca. 25 Personen anwesend." Als Ereignis ist zu lesen: „friedliche Demoaktion". Dennoch werden Vorname, Nachname, Anschrift und Mobilfunknummer von zwei Versammlungsteilnehmern (verantwortliche Personen) erfasst und gespeichert.

Erfreulicherweise hat meine Prüfungsmaßnahme dazu geführt, dass bisher insgesamt 376 vergleichbare Datensätze von Versammlungsteilnehmern im polizeilichen Vorgangsbearbeitungssystem NIVADIS gelöscht wurden. Ich werde darauf drängen, dass auch bei der PD Lüneburg eine entsprechende Löschung vorgenommen wird.

Zum Ende des Berichtszeitraums war die von der Landesregierung[2] angekündigte erneute vollständige Überprüfung der bei der PD Lüneburg gespeicherten Datensätze noch nicht abgeschlossen. Im nachfolgenden Tätigkeitsbericht werde ich über das abschließende Ergebnis dieser datenschutzrechtlichen Prüfung berichten.

1 LT-Drs. 17/7320

2 LT-Drs. 17/7320, Antwort auf die Frage 4

1.9 Prüfung der bundesweiten Falldatei Rauschgift durch die Datenschutzbeauftragten des Bundes und der Länder

Unstrukturierte Dokumentation von Speichervoraussetzungen, unzureichende Verdachtsmomente oder ungenügende Prüfungen für die Speicherung von personenbezogenen Daten. Bei einer Prüfung der Falldatei Rauschgift haben die Datenschutzbeauftragten des Bundes und der Länder eine Reihe von Datenschutzverstößen festgestellt.

Die Falldatei Rauschgift ist eine bundesweite Verbunddatei, in der Informationen über sichergestellte Drogen und Verstöße gegen das Betäubungsmittelgesetz gespeichert werden. Sie wird auf Grundlage des Bundeskriminalamtgesetzes (BKAG) zentral beim Bundeskriminalamt geführt. Die Polizeien der Länder und die Zollfahndung haben Zugriff auf die Datei und können direkt Daten einspeichern und abrufen. Die datenschutzrechtliche Verantwortung für die Verarbeitung der personenbezogenen Daten liegt grundsätzlich bei dem Landeskriminalamt des Bundeslandes, das die Speicherung in der Falldatei vornimmt.

Eine gemeinsame Prüfung des Datenbestandes durch die Bundes- und die Landesbeauftragten für den Datenschutz hat im Wesentlichen folgende Mängel aufgedeckt:

Vielfach haben die Behörden nicht ausreichend geprüft, ob die Voraussetzungen für eine Datenspeicherung nach § 2 BKAG (Straftat von länderübergreifender oder erheblicher Bedeutung) und nach § 8 Abs. 2 BKAG (Negativprognose) vorliegen. Verbreitet fehlt es an einer nachvollziehbaren Dokumentation des Vorliegens der gesetzlichen Speichervoraussetzungen. Somit wurden vielfach Speicherungen festgestellt, die dem Bereich der Bagatellkriminalität zuzuordnen sind und keine bundesweite Relevanz besitzen. Auch wurden Personen gespeichert, bei denen kein hinreichender polizeilicher Restverdacht festzustellen war. Das Ergebnis des jeweiligen Strafverfahrens war bei vielen Einträgen nicht berücksichtigt – entweder aufgrund organisatorischer Mängel oder weil die nach § 482 Abs. 2 Strafprozessordnung notwendige Mitteilung der Staatsanwaltschaft unterblieb.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder fordert in einer gemeinsamen Entschließung vom 10. November 2016 (92. Konferenz in Kühlungsborn)[1] nicht nur in der Falldatei Rauschgift bestehende Mängel zu beseitigen, sondern die Einhaltung grundlegender Standards bei jedweder Speicherung in Verbunddateien der Polizei sicherzustellen.

1 http://www.lfd.niedersachsen.de/download/112518

Die personenbezogenen Daten aus der Falldatei Rauschgift dürfen nicht ohne Einzelfallprüfung in die neue Datei Betäubungsmittelkriminalität im Polizeilichen Informations- und Analyseverbund (PIAV) aufgenommen werden, die voraussichtlich noch im Jahr 2017 die Falldatei Rauschgift ablösen wird.

Keine Mängel beim Landeskriminalamt Niedersachsen

Im Landeskriminalamt Niedersachsen erfolgte durch uns eine auszugsweise Prüfung von 20 Datensätzen aus der durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zur Verfügung gestellten Stichprobenmenge. Hierbei wurde bewusst auf eine Vorselektion der Prüfdatensätze hinsichtlich einzelner Straftatbestände und/oder Tatbestandsmerkmale verzichtet, um ein möglichst realistisches Abbild des Speicherverhaltens bzw. der Speicherkriterien zu erhalten. Die Mängel, die in nahezu allen anderen Bundesländern festgestellt wurden, lagen im Landeskriminalamt Niedersachsen nicht vor.

Allen Fällen lagen Straftaten von länderübergreifender oder erheblicher Bedeutung zugrunde, die eine Verarbeitung in der Falldatei rechtfertigten. Die Dokumentation jedes einzelnen Prüffalles war nachvollziehbar und völlig ausreichend. Sämtliche personenbezogenen Daten waren dem Personenstatus „Beschuldigter“ zuzuordnen, so dass ein entsprechender polizeilicher Verdacht zu begründen war. In allen Fällen war das Ergebnis des jeweiligen Strafverfahrens vermerkt und somit im Fall eines Abrufs erkennbar.

Im Zuge unseres durchgeführten Prüfverfahrens ergaben sich keinerlei Anhaltspunkte dafür, den datenschutzkonformen Umgang der Polizei Niedersachsen mit personenbezogenen Daten im Zusammenhang mit der Falldatei Rauschgift in Abrede zu stellen und die Prüfung auf einen weitergehenden Datenbestand auszudehnen.

1.10 LfD Niedersachsen beanstandet mangelhafte Auskunft bei der Polizei

Im Rahmen einer Bürgereingabe erhielt ich Kenntnis von einer mangelhaften und damit rechtswidrigen Auskunft über polizeilich gespeicherte Daten. Zu diesem Vorgang habe ich eine förmliche Beanstandung ausgesprochen.

Mein Petent bat das Landeskriminalamt Niedersachsen (LKA NI) im Oktober 2012 um eine umfassende Auskunft zu den zu seiner Person gespeicherten personenbezogenen Daten, insbesondere in den polizeilichen Systemen „POLAS“[1] und „NIVADIS“[2]. Seinem Antrag ist zu entnehmen, dass sich die Auskunft auf alle bei der Polizei Niedersachsen gespeicherten Daten erstrecken sollte.

Der behördliche Datenschutzbeauftragte des LKA NI antwortete meinem Petenten im November 2012 und teilte ihm mit, dass beim LKA NI keine Speicherungen zu seiner Person vorhanden seien. Verantwortliche Stelle und damit zuständig für die Beantwortung seines Auskunftsersuchens sei die Polizeidirektion (PD) Hannover. Gleichzeitig wurde das Auskunftsersuchen zuständigkeitshalber an die PD Hannover weitergeleitet mit dem Hinweis, dass neben den Verarbeitungen im Vorgangsbearbeitungssystem NIVADIS auch eine Verarbeitung in der Anwendung „SAFIR“[3] gespeichert sei.

Trotz dieses Hinweises des LKA NI bezog sich die Auskunft des Datenschutzbeauftragten der PD Hannover an meinen Petenten ausschließlich auf die Verarbeitungen seiner personenbezogenen Daten im Vorgangsbearbeitungssystem „NIVADIS“. Ein Hinweis auf mögliche andere Verarbeitungen in anderen Systemen der Polizei erfolgte nicht. Damit war die Auskunft fehlerhaft.

Ein Auskunftsanspruch bezieht sich immer auf den kompletten Datenbestand der durch die verantwortliche Stelle zum Zeitpunkt der Antragstellung vorgehalten wird. Nur durch eine vollständige Auskunft werden die im sog. Volkszählungsurteil[4] verankerten Aufklärungs- und Auskunftspflichten erfüllt.

Im September 2015 stellte mein Petent erneut ein Auskunftsersuchen nach § 16 NDSG gegenüber der Polizeidirektion Hannover. Der behördliche Datenschutzbeauftragte antwortete ihm im Mai 2016 detailliert und erwähnte dabei auch die Verarbeitung von Daten in der Fallbearbeitungssoftware SAFIR, über die seinerzeit keine Auskunft erteilt worden war. Ferner enthielt das Schreiben den Hinweis: „Neben der o. g. Erfassung im Vorgangsbearbeitungssystem ‚NIVADIS‘ sind Sie in der Fallbearbeitungssoftware ‚SAFIR‘ gespeichert gewesen.“

1 POLAS = polizeiliches Auskunftssystem auf Landesebene

2 NIVADIS = Niedersächsisches Vorgangsbearbeitungs-, Auskunfts-, Dokumentations- und Informationssystem der Polizei

3 SAFIR = Software zur Analyse, Fallbearbeitung, Informationsverarbeitung und Recherche der Polizei

4 Urteil des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65,1)

Polizeidirektion löscht rechtswidrig erhobene Daten nach Petentenanfrage

Dieser Hinweise veranlasste meinen Petenten dazu, die physikalische Löschung seiner Daten in der Fallbearbeitungssoftware „SAFIR" im Verlauf seines Auskunftsbegehrens von mir überprüfen zu lassen. Ich habe daraufhin die PD Hannover im September 2016 um eine Stellungnahme zu den Umständen der physikalischen Löschung der personenbezogenen Daten in der Anwendung „SAFIR" gebeten. Dabei stellte sich heraus, dass die Daten unmittelbar nach Eingang des Auskunftsersuchens gelöscht worden waren. Dieses Vorgehen ist ebenfalls datenschutzrechtlich nicht hinnehmbar. Es widerspricht der geltenden Rechtslage. Stellt die öffentliche Stelle im Zusammenhang mit einem Auskunftsersuchen nach § 16 NDSG fest, dass die Daten nicht hätten gespeichert werden dürfen oder zur Aufgabenerfüllung nicht mehr erforderlich sind, darf sie diese Daten nicht ohne weiteres löschen. Sie muss vielmehr zunächst den Auskunftsanspruch erfüllen, dem Betroffenen die Daten mitteilen und ihn auf ihre Löschungsabsicht hinweisen.

Polizei prüft landeseinheitlichen Umgang mit Auskunftsersuchen

Das Verhalten der PD Hannover, nämlich die unvollständige Auskunftserteilung im Rahmen des ersten Auskunftsersuchens und in der Folge die Löschung der gespeicherten Daten in „SAFIR" während des laufenden zweiten Auskunftsersuchens, führt im Ergebnis zu einem erheblichen datenschutzrechtlichen Verstoß. Ich habe daher eine förmliche Beanstandung nach § 23 Abs. 1 NDSG gegenüber dem Ministerium für Inneres und Sport im Dezember 2016 ausgesprochen.

In der Beanstandung habe ich ferner darum gebeten, durch geeignete Maßnahmen dafür Sorge zu tragen, dass zukünftig derartige Löschungen im Rahmen eines Auskunftsbegehrens unterbleiben, um die Rechte der Betroffenen zu wahren. Sind die Daten gelöscht, hat die betroffene Person keine Möglichkeit mehr, die Rechtmäßigkeit des Datensatzes überprüfen zu lassen.

Ferner bat ich um Stellungnahme, wie zukünftig sichergestellt werden soll, dass bei einem Antrag auf Auskunft gemäß § 16 NDSG, der sich auf alle Verarbeitungen einer verantwortlichen Stelle bezieht, neben den Auskünften aus dem Vorgangsbearbeitungssystem „NIVADIS" auch Auskunft zu anderen polizeilichen Datenbanken wie z. B. „POLAS" oder „SAFIR" und zu personenbezogenen Inhalten einer polizeilichen Einsatzleitsoftware erteilt wird.

Das Niedersächsische Ministerium für Inneres und Sport hat zwischenzeitlich reagiert und durch Erlass die Polizeidirektionen angewiesen, zukünftig polizeilich gespeicherte Daten während eines laufenden Auskunftsersuchens nicht zu löschen. Ferner wurde im Kreis der behördlichen Datenschutzbeauftragten der Polizeibehörden eine Arbeitsgruppe eingerichtet, die Wege und Möglichkeiten aufzeigen soll, wie zukünftig polizeiliche Auskunftsersuchen von Bürgerinnen und Bürgern landeseinheitlich und vor allem vollständig beantwortet werden können.

Ich werde die Vorschläge und Ergebnisse der Arbeitsgruppe unter dem Gesichtspunkt der Stärkung der Betroffenenrechte gegenüber den Polizeibehörden intensiv prüfen.

1.11 Prüfung einer nicht-individualisierten Funkzellenabfrage

Sind Personen im Rahmen einer Funkzellenabfrage von einer polizeilichen Datenerhebung betroffen, müssen sie nachträglich informiert werden. Nur auf diese Weise kann die Rechtmäßigkeit der Maßnahmen überprüft werden. Häufig geschieht dies jedoch nicht, wie der hier vorgestellte Fall verdeutlicht.

Im März 2016 bat mich der bevollmächtigte Rechtsanwalt eines Petenten um die datenschutzrechtliche Prüfung der Verarbeitung personenbezogener Daten aus Anlass strafrechtlicher Ermittlungen im Zusammenhang mit einer gefährlichen Körperverletzung zum Nachteil zweier junger Männer in Osnabrück. Die Opfer gaben an, dass ihnen aus einer Gruppe von ca. vier bis sieben Personen heraus Reizgas in das Gesicht gesprüht worden sei. Die Polizei vermutete, dass die Täter der linken Szene angehören.

Die Staatsanwaltschaft erwirkte einen richterlichen Beschluss für eine sog. Funkzellenauswertung nach § 100g StPO. In einem Radius von 500 Metern um den Tatort herum wurden insgesamt 14.269 Datensätze bei Telekommunikationsanbietern erhoben, die durch eine nachträgliche Filterung auf 778 Rufnummern begrenzt werden konnten. Die Rufnummern wurden den Anschlussinhabern zugeordnet und mit weiteren Datenbanken der Polizei abgeglichen, in denen Personen gespeichert sind, die aufgrund zurückliegender polizeilich registrierter Vorfälle dem gewaltbereiten, linksextremistischen Spektrum zugeordnet werden können. Dieser Abgleich mit den polizeilichen Datenbanken führte zu insgesamt sieben tatverdächtigen Personen. Bei diesen Personen fanden auf der Grundlage richterlicher Beschlüsse Wohnungsdurchsuchungen statt, um den Tatverdacht durch Beweismittel konkretisieren zu können.

Ich habe dem Rechtsanwalt zunächst verdeutlicht, dass mir eine Überprüfung der Rechtmäßigkeit der ergangenen Beschlüsse zur Funkzellenauswertung und Wohnungsdurchsuchung wegen der richterlichen Unabhängigkeit nach dem Datenschutzgesetz nicht möglich ist. Meine datenschutzrechtliche Prüfung beschränkte sich daher nur auf die Frage, ob der betroffene Mandant von den Strafverfolgungsbehörden ordnungsgemäß über die Funkzellenabfrage benachrichtigt und über seine Rechte belehrt wurde.

Betroffene nur unzureichend informiert

Nach Einsichtnahme in die Ermittlungsakten konnte ich dem Beschluss zur Wohnungsdurchsuchung entnehmen, dass dort beiläufig in den Gründen auf eine vorab durchgeführte Funkzellenabfrage hingewiesen wurde. Dies ist aus

datenschutzrechtlicher Sicht nicht ausreichend, denn der Gesetzgeber verlangt eine ausdrückliche Benachrichtigung und Rechtsbehelfsbelehrung.

Gemäß § 101 a Abs. 6 i. V. m. § 101 StPO sind die von einer Verkehrsdatenerhebung im Rahmen einer Funkzellenabfrage betroffenen Personen grundsätzlich nachträglich zu benachrichtigen. Gesetzlich normierte Ausnahmetatbestände von der Benachrichtigungspflicht kommen jedenfalls dann nicht in Betracht, wenn sich auf der Grundlage einer Funkzellenabfrage weitere Ermittlungsmaßnahmen wie eine Wohnungsdurchsuchung anschließen. Die Benachrichtigung umfasst auch den Hinweis auf einen nachträglich möglichen Rechtsschutz unter Nennung der zweiwöchigen Frist nach § 101 Abs. 7 StPO. Benachrichtigung und Rechtsbehelfsbelehrung gewährleisten den subjektiven Rechtsschutz des Betroffenen. Gleichzeitig wird so die Transparenz der eingesetzten Ermittlungsmaßnahme sichergestellt. Von einer Funkzellenabfrage erfahren die Betroffenen in der Regel nichts. Umso wichtiger ist es, dass durch eine ausdrückliche Benachrichtigung und Rechtsbehelfsbelehrung die betroffene Person die Möglichkeit erhält, nachträglich die Rechtmäßigkeit einer Datenerhebung und –verarbeitung gerichtlich überprüfen zu lassen.

Landesbeauftragte für den Datenschutz unterstützt Einführung einer aussagekräftigen Statistik

Die Thematik „Funkzellenabfrage" war im Berichtszeitraum auch Gegenstand parlamentarischer Beratungen. Mit einem Entschließungsantrag forderte die Fraktion der FDP[1], eine Statistik zu nicht-individualisierten Funkzellenabfragen mit folgenden Inhalten zu erstellen:

- die Anzahl der beantragten und der genehmigten Funkzellenabfragen,
- eine Aufschlüsselung nach Polizeibehörden, die die Maßnahme beantragt haben,
- die zugrundeliegenden Straftatbestände bei der Beantragung,
- die jeweilige Anzahl der betroffenen Telekommunikationsanschlüsse,
- die Anzahl der Verfahren, in denen die Funkzellendaten verwendet bzw. eingebracht wurden,
- die Dauer der Speicherung der jeweiligen Daten.

Im Rahmen einer Anhörung im Oktober 2016 im Ausschuss für Inneres und Sport habe ich dieses Anliegen grundsätzlich unterstützt. Die Einführung einer aussagekräftigen Statistik über nicht-individualisierte Funkzellenabfragen im Rahmen der Strafverfolgung (§ 100g Abs. 3 StPO) ist verfassungsrechtlich geboten. Ich halte vor dem Hintergrund der Rechtsprechung des Bundesverfassungsgerichts[2] die Regelung des § 101b StPO zur Statistikpflicht für unzureichend und damit für verfassungsrechtlich bedenklich. Wesentliche Angaben finden keinen Eingang in diese Statistik, z. B. zur Anzahl der betroffenen Telekommunikationsanschlüsse und der erhobenen Verkehrsdatensätze. Diese Angaben sind aber unerlässlich, um die vom Bundesverfassungsgericht geforderte nachträgliche demokratische Kontrolle und Überprüfung von heimlich durchgeführten Ermittlungsmaßnahmen durch Parlament und Öffentlichkeit sicherstellen zu können. So fordert das Bundesverfassungsgericht unter dem Gesichtspunkt der Transparenz und Kontrolle:

> „Da sich die Durchführung von heimlichen Überwachungsmaßnahmen der Wahrnehmung der Betroffenen und der Öffentlichkeit entzieht und dem auch Benachrichtigungspflichten oder Auskunftsrechte mit der Möglichkeit anschließenden subjektiven Rechtsschutzes nur begrenzt entgegenwirken können, sind hinsichtlich der Wahrnehmung dieser Befugnisse regelmäßige Berichte des Bundeskriminalamts gegenüber Parlament und Öffentlichkeit gesetzlich sicherzustellen. Sie sind erforderlich und müssen hinreichend gehaltvoll sein, um eine öffentliche Diskussion über Art und Ausmaß der auf diese Befugnisse gestützten Datenerhebung, einschließlich der Handhabung der Benachrichtigungspflichten und Löschungspflichten, zu ermöglichen und diese einer demokratischen Kontrolle und Überprüfung zu unterwerfen."

Bei der Funkzellenabfrage handelt es sich um eine verdeckt durchgeführte Ermittlungsmaßnahme, denn die Betroffenen werden im Vorfeld der Maßnahme nicht informiert. Dies ist in der Regel auch gar nicht möglich, denn es bleibt dem Zufall überlassen, welche Personen sich zum Zeitpunkt der Datenerhebung im örtlichen Einzugsgebiet der Funkzelle aufhalten.

1 LT-Drs. 17/5822

2 BVerfGE 141, 220-378

Hinzu kommt, dass die Betroffenen in der Regel auch nicht nachträglich von der Maßnahme unterrichtet werden, da die Staatsanwaltschaften nach § 101 Abs. 4 Satz 4 StPO in der Regel von der gesetzlich verankerten Pflicht zur Benachrichtigung der Betroffenen absehen. Eine gerichtliche Überprüfung findet daher bei nicht-individualisierten Funkzellenabfragen regelmäßig nicht statt; die Rechtsschutzmöglichkeiten der Betroffenen sind damit verkürzt.

Grundrechtsschutz rechtfertigt höheren Arbeitsaufwand in Behörden

Umso wichtiger ist in diesen Fällen eine aussagekräftige und gehaltvolle Statistik, die es ermöglicht, dass sowohl im parlamentarischen Raum als auch in der Öffentlichkeit eine fundierte Diskussion über den Einsatz nicht-individualisierter Funkzellenabfragen zur Strafverfolgung durch die Sicherheitsbehörden stattfinden kann. Angaben zur Anzahl der Verfahren und Erstanordnungen bzw. Verlängerungsanordnungen allein sind unzureichend und erfüllen die Vorgaben des Bundesverfassungsgerichts nur ansatzweise. Zwingend erforderlich ist aus Sicht des Datenschutzes die Angabe zur Anzahl der von einer nicht-individualisierten Funkzellenabfrage betroffenen Bürgerinnen und Bürger.

Die Anzahl der Betroffenen ist ein wesentliches Kriterium im Rahmen der Verhältnismäßigkeitsprüfung bei der Anordnung der Maßnahme. Gleiches muss im Nachgang einer nicht-individualisierten Funkzellenabfrage gelten, wenn es darum geht, transparent und auf fundierter Tatsachenbasis zwischen Abgeordneten oder in der Öffentlichkeit zu diskutieren, ob die Strafverfolgungsbehörden von der nicht-individualisierten Funkzellenabfrage angemessen Gebrauch gemacht haben.

Der immer wieder gern vorgebrachte Einwand des mit einer erweiterten Statistik verbundenen Aufwandes bei den Sicherheitsbehörden ist verfassungsrechtlich unbeachtlich. Ist Mehraufwand zur Absicherung von Grundrechten erforderlich, so ist dieser von den Behörden zu leisten. Darüber hinaus dürfte sich der Mehraufwand auch in Grenzen halten. Die im Entschließungsantrag geforderten Angaben sind ohne weiteres den Ermittlungsakten zu entnehmen. Hinzu kommt, dass diese Angaben auch erforderlich sind, um die Anordnung und Durchführung der nicht-individualisierten Funkzellenabfrage so zu dokumentieren, dass eine nachträgliche datenschutzrechtliche Kontrolle jederzeit möglich ist.

Der Entschließungsantrag wurde im Ausschuss und in der abschließenden Beratung im Plenum mit der Mehrheit der Regierungsfraktionen abgelehnt. Seit Jahren verweigert die Landesregierung beharrlich die verfassungsrechtlich gebotene Transparenz bei Funkzellenabfragen zur Strafverfolgung nach § 100g StPO.[3] Der Regierungswechsel 2013 hat daran bedauerlicherweise nichts geändert. Andere Länder, wie z. B. Schleswig-Holstein, sind hier wesentlich weiter. Dort macht die Landesregierung inzwischen detaillierte Angaben zur Durchführung von Funkzellenabfragen.[4]

3 LT-Drs. 16/3876; 17/1160; 17/2055

4 Vgl. hierzu Schleswig-Holsteinischer Landtag, Drs. 18/1021

2. Allgemeine Landesverwaltung und

2.1 Schwerpunktprüfung Fahrerlaubnisbehörden: Grundsätzlich ein positives Bild

Hinweise auf datenschutzrechtliche Mängel in einer Fahrerlaubnisbehörde nahm ich zum Anlass für eine landesweite Überprüfung aller Einrichtungen in Niedersachsen. Überprüft wurden unter anderem der technisch-organisatorische Datenschutz sowie der Ausbildungsstand der behördlichen Datenschutzbeauftragten.

Für eine Beratung zu einer Videoüberwachung in einer niedersächsischen Stadtverwaltung wurden u. a. die dortigen Räume der Fahrerlaubnisbehörde aufgesucht. Die dort angetroffenen Mitarbeiterinnen und Mitarbeiter der Stadtverwaltung machten unaufgefordert auf datenschutzrechtliche Probleme aufmerksam, die mit dem eigentlichen Beratungsgegenstand „Videoüberwachung“ nichts zu tun hatten. Berichtet wurde insbesondere über Probleme mit der räumlichen Situation, die eine datenschutzgerechte Bearbeitung der Fahrerlaubnisangelegenheiten nicht zuließe. Den Bürgerinnen und Bürgern wurde die Möglichkeit ein vertrauliches Einzelgespräch zu führen nicht angeboten. So mussten Angaben zur Wiedererlangung der Fahrerlaubnis, die teilweise sensible Gesundheitsdaten (beispielsweise strafrechtlich relevantes Verhalten oder Suchtprobleme) beinhalteten, vor einer Vielzahl anderer Personen abgegeben werden.

Dieser Fall gab den Anstoß zu einer landesweiten datenschutzrechtlichen Überprüfung aller 63 Fahrerlaubnisbehörden in Niedersachsen. Mittels eines Fragebogens wurde der technisch-organisatorische Datenschutz beim Umgang mit besonders sensiblen personenbezogenen Daten (Gesundheitsdaten/Strafverfahren), die räumlichen Bedingungen vor Ort sowie der Aus- und Fortbildungsstand der behördlichen Datenschutzbeauftragten und der Mitarbeiterinnen und Mitarbeiter in Bezug auf die Anwendung der datenschutzrechtlichen Regelungen überprüft.

Keine gravierenden Mängel

Nach Auswertung der Fragebögen zeigte sich insgesamt ein erfreuliches Bild. Flächendeckende gravierende datenschutzrechtliche Mängel waren bei den 63 Fahrerlaubnisbehörden nicht festzustellen. Vereinzelt wurden den Behörden im bilateralen Wege Lösungen aufgezeigt, um eine unmittelbare Mängelbeseitigung zu ermöglichen.

Kommunen

Insbesondere wurde hier empfohlen, bessere Möglichkeiten für eine vertrauliche Gesprächsführung durch die Einrichtung von Einzelbüros zu schaffen. Schon während der Anmeldung zu einem Termin sollten die betroffenen Bürgerinnen und Bürger auf diese Möglichkeit hingewiesen werden. Auch wurden konkrete Empfehlungen für eine datenschutzkonforme Verarbeitung der dort vorgehaltenen digitalen und analogen Datenbestände gegeben. So sollte der Zugang zu elektronischen Anwendungen nur über einen ausreichenden Passwortschutz ermöglicht werden. Hier habe ich entsprechende Vorschläge zu einer sicheren Passwortgestaltung in Anlehnung an die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik gemacht.

Schließlich wurden die behördlichen Datenschutzbeauftragten an ihre aus § 8a NDSG abzuleitende Verpflichtung erinnert, für eine Aus- und Fortbildung der Mitarbeiterinnen und Mitarbeiter Sorge zu tragen. Auch die behördlichen Datenschutzbeauftragten müssen speziell geschult sein, um eine datenschutzgerechte Bearbeitung von Fahrerlaubnisangelegenheiten in der räumlichen Situation von Großraumbüros sicherstellen und überprüfen zu können.

2.2 Ordnungswidrigkeiten-Verfahren bei Datenschutzverstößen: Geringe Ahndungsqoute in Landesverwaltung und Kommunen

Trotz zahlreicher Eingaben und umfassender Sanktionsmöglichkeiten wurden in Landesverwaltung und Kommunen zwischen 2014 und 2016 nur wenige Ordnungswidrigkeit-Verfahren nach Datenschutzverstößen durchgeführt. Zu diesem überraschenden Ergebnis kommt eine Erhebung im Berichtszeitraum.

Die ab Mai 2018 unmittelbar geltende europäische Datenschutz-Grundverordnung (DS-GVO) stärkt die Rechte der Betroffenen im Hinblick auf den Schutz ihrer Daten und stellt den Aufsichtsbehörden zur Rechtsdurchsetzung und zur Ahndung von datenschutzrechtlichen Verstößen ein breites Spektrum an Maßnahmen zur Verfügung. Neben den in Artikel 58 Abs. 2 DS-GVO genannten Abhilfebefugnissen, wie z. B. Verwarnungen und Anweisungen, können die Aufsichtsbehörden datenschutzrechtliche Verstöße nach Artikel 83 DS-GVO auch mit Geldbußen ahnden. Damit sendet die DS-GVO das unmissverständliche Signal aus, dass datenschutzrechtliche Verstöße zukünftig konsequenter und mit spürbarer Wirkung für die Betroffenen geahndet werden sollen.

Nicht länger zahnloser Tiger – DS-GVO stärkt Position des Datenschutzes

Aufgrund der Öffnungsklausel des Artikels 83 Abs. 7 DS-GVO kann national geregelt werden, ob und in welchem Umfang nicht nur gegen Unternehmen, sondern auch gegen Behörden und sonstige öffentliche Stellen Geldbußen bei Datenschutzverstößen verhängt werden können. Diese Ausweitung der möglichen Sanktionsmaßnahmen auf den öffentlichen Bereich entspricht einer Forderung der Datenschutz-Aufsichtsbehörden, der seitens des nationalen Gesetzgebers bislang nicht entsprochen wurde. Die Verhängung von Geldbußen auch gegenüber dem öffentlichen Bereich ist nach den bisherigen Erfahrungen der Datenschutz-Aufsichtsbehörden von gleicher Relevanz, wie die bereits festgelegten Bußgeldregelungen für den nicht-öffentlichen Bereich. Dies würde die bisherige Besserstellung der öffentlichen Verwaltung gegenüber der freien Wirtschaft aufheben. Zudem würde die Position der oftmals als „zahnlose Tiger“ bezeichneten Datenschutz-Aufsichtsbehörden gestärkt werden.
Zum Schutz der Betroffenen gegen bestimmte Formen des unbefugten Umgangs mit ihren personenbezogenen Daten gab es bereits im Berichtszeitraum geltenden NDSG Sanktionsregelungen zu Bußgeld- und Strafverfahren: Soweit es sich bei einem Verstoß gegen datenschutzrechtliche Regelungen

nicht um eine Straftat nach bereichsspezifischen Strafnormen (s. z. B. § 203 Strafgesetzbuch) oder nach § 28 NDSG handelt, bedarf es seitens der zuständigen Behörden und sonstigen öffentlichen Stellen stets der Prüfung, ob der Verstoß als Ordnungswidrigkeit gemäß § 29 NDSG zu ahnden ist. Beispiele aus der Praxis: Ein Bediensteter der Personalstelle einer Behörde offenbart vertraulich zu handhabende dienstliche Informationen, wie z. B. Details zu einem laufenden Personalauswahlverfahren abends am Stammtisch gegenüber Freunden (= unbefugte Dritte). Oder eine Beschäftigte einer Kommune erzählt einem Bürger in einem Telefongespräch, welche Person ihn bei der Kommunalverwaltung „angeschwärzt" hat. Beide Male läge ein Verstoß gegen das Datengeheimnis nach § 5 NDSG vor, der mit einer Ordnungswidrigkeit zu ahnden wäre.

Da die DS-GVO bei Verletzungen des Schutzes personenbezogener Daten umfangreiche Dokumentations- und weitgehende Meldepflichten der Verantwortlichen gegenüber den Aufsichtsbehörden vorsieht (siehe u. a. Art. 33 DS-GVO), ist für die Ressourcenplanung der Behörden und öffentlichen Stellen die weitere Entwicklung im Bereich der Sanktionen von Belang. Eine landesweite Statistik, wie viele Ordnungswidrigkeiten-Verfahren gegen datenschutzrechtliche Verstöße es in den letzten Jahren im Bereich der Landes- oder Kommunalverwaltung gab, wird aktuell nicht geführt.

Nur geringe Zahl von Bußgeldverfahren

Um den Status quo zu ermitteln, habe ich 2016 als ersten Schritt eine Abfrage bei den für Ordnungswidrigkeiten-Verfahren zuständigen Behörden im kommunalen Bereich zu den durchgeführten Ordnungswidrigkeiten-Verfahren nach § 29 NDSG vorgenommen. Zu meiner großen Verwunderung hat diese ergeben, dass in den Jahren 2014 bis 2016 fast gar keine Verfahren durchgeführt wurden. Von 47 angeschriebenen Kommunen haben lediglich zwei Kommunen Fälle gemeldet, in denen Bußgelder festgesetzt worden sind (insgesamt 3 Fälle), ein weiteres Verfahren wurde eingestellt.

Aufgrund der Vielzahl der bei mir eingehenden Anfragen und Eingaben ist davon auszugehen, dass es in der Praxis zu weitaus mehr datenschutzrechtlichen Verstößen kommt, als letztendlich geahndet werden. Über die Hintergründe der aus meiner Sicht sehr zurückhaltenden Ahndungspraxis kann ich nur spekulieren. Möglicherweise sind die bestehende Ahndungsvorschrift des § 29 NDSG und die Festlegung der fachlichen Zuständigkeit für Datenschutzverstöße in der Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten(ZustVO-OWi) zu wenig bekannt.

Selbst unter der Prämisse, dass die Verantwortlichen im kommunalen Bereich den Schwerpunkt im Bereich Datenschutz in den letzten drei Jahren in der Vorbeugung, sprich in der Aufklärung und Beratung ihrer Beschäftigten zu datenschutzrechtlichen Vorgaben gesetzt haben, ist es nicht zu erklären, dass es im gesamten Land fast keine ahndungswürdigen Verstöße gegen datenschutzrechtliche Vorschriften gab.

Bei Vorstellung des Ergebnisses meiner Abfrage bei den Netzwerken der behördlichen Datenschutzbeauftragten wurden verschiedene Aspekte deutlich, die in diesem Zusammenhang von Belang sind: Oftmals ist die personelle Ausstattung für interne Datenschutz-Kontrollen und für die im Allgemeinen arbeitsintensiven Bußgeldverfahren im kommunalen Bereich nicht ausreichend. In der Praxis sind die meisten behördlichen Datenschutzbeauftragten, denen –„wenn überhaupt"– datenschutzrechtliche Verstöße zugetragen werden, nur zu einem geringfügigen Anteil von ihren sonstigen „Linienaufgaben" freigestellt. Das vorhandene Personal, insbesondere der Bußgeldstellen, soll nicht zusätzlich zu den sonstigen wahrzunehmenden Aufgaben auch noch mit Datenschutz-Fällen belastet werden. Hinzu kommt die Sichtweise, dass sich die Verantwortlichen vor ihre Beschäftigten stellen und diese vor möglichen Konsequenzen ihrer Handlungsweisen schützen („Menschen sind keine Maschinen und machen Fehler, es sind doch nur Datenschutz-Verstöße").

Begehen Landes- oder Kommunalbedienstete datenschutzrechtliche Verstöße, so sind diese mit Blick auf die DS-GVO konsequenter als bisher zu verfolgen und zu ahnden. Ferner ist eine meiner Forderungen bei der anstehenden Anpassung des niedersächsischen Datenschutzrechts an die DS-GVO, dass der niedersächsische Gesetzgeber auch für den öffentlichen Bereich die Bußgeldregelungen verschärfen muss. Vom neuen NDSG hat die klare Botschaft auszugehen, dass zukünftig datenschutzrechtliche Verstöße keine Kavaliersdelikte sind.

Im Rahmen der mir als Aufsichtsbehörde obliegenden Kontrollaufgaben (s. Art. 58 Abs. 2 lit. b) DS-GVO) werde ich zu einem späteren Zeitpunkt erneut eine landesweite Erhebung zu durchgeführten Ordnungswidrigkeiten-Verfahren vornehmen, um zu überprüfen, ob sich die Sanktionierungspraxis im Landes- als auch im Kommunalbereich im Vergleich zum Status quo verbessert hat.

2.3 "Deutschland-Cloud" – Dialog mit einer niedersächsischen Behörde

In meinen beiden vorherigen Tätigkeitsberichten habe ich über grundsätzliche Probleme und Lösungsansätze für ein datenschutzrechtlich ordnungsgemäßes Cloud Computing als eine moderne Form der Auftragsdatenverarbeitung berichtet. Im Berichtszeitraum hatte ich nunmehr Gelegenheit, mich mit einem konkreten Anwendungsfall einer Cloud-Computing-Lösung im Geschäftsbereich des Niedersächsischen Justizministeriums (MJ) datenschutzrechtlich auseinanderzusetzen.

Im Rahmen eines größeren IT-Projektes hatte eine niedersächsische Behörde in Erwägung gezogen, Rechenleistung und damit die Verarbeitung personenbezogener Daten in Form der vom Anbieter Microsoft als besonders sicher und datenschutzkonform beworbenen Plattform „Deutschland-Cloud" einzukaufen. Aufgrund noch offener datenschutzrechtlicher Fragen hat mich die Behörde frühzeitig beratend in ihre Entscheidungsfindung einbezogen. Dadurch war es möglich, datenschutzrechtliche Problempunkte im vorliegenden Vertragswerk direkt im Gespräch mit dem Anbieter aufzuzeigen und zu erörtern.

Bei den bisher am Markt angebotenen Cloud-Produkten besteht das grundsätzliche Problem, dass US-Gesetze amerikanische Unternehmen wie Microsoft verpflichten, auch die in europäischen Rechenzentren gespeicherten Daten an US-Sicherheitsbehörden herauszugeben. Die Herausgabepflicht trifft nicht nur den Mutterkonzern mit Sitz in den USA, sondern auch die Tochtergesellschaften, die Rechenzentren in Europa betreiben. In welchem Umfang US-Sicherheitsbehörden von diesen Datenzugriffsrechten Gebrauch machen, bleibt der Öffentlichkeit weitestgehend verborgen, weil die Provider im Falle einer Herausgabe-Anordnung zur Verschwiegenheit verpflichtet sind.

Zahlreiche Unklarheiten bei Microsoft-Cloud

Mit der „Deutschland-Cloud" verspricht der Anbieter dem Kunden, dass dessen Daten vor dem Zugriff durch US-Sicherheitsbehörden geschützt seien. Dies solle dadurch erreicht werden, dass im Unterschied zu den bisherigen Microsoft-Cloud-Diensten der Betreiber des in Deutschland stehenden Rechenzentrums eine deutsche Firma (T-Systems) ist, die als Datentreuhänder fungiere. Das Unternehmen T-Systems ist ein „virtueller Türsteher" des Rechenzentrums, ohne dessen Mitwirkung es Microsoft-Mitarbeitern verwehrt sei, direkt oder per Fernwartung auf die Daten in Deutschland zuzugreifen. Auch US-Behörden könnten auf Daten des Rechenzentrums nur zugreifen,

wenn dies nach deutschem Recht und den Treuhandvereinbarungen zulässig wäre. Letztlich versprechen Microsoft und T-Systems ihren Kunden, dass T-Systems als Datentreuhänder jeden physischen und technischen Zugriff auf die Kundendaten überwache und kontrolliere. Ausnahme hiervon stelle lediglich der Zugriff durch den Kunden selbst dar. Zudem würden die Daten ausschließlich innerhalb Deutschlands gespeichert und transferiert.

Nach Durchsicht der mir überlassenen Unterlagen und nach Vorstellung des Produktes im Februar 2016 durch Vertreter der Fa. Microsoft ergaben sich für mich zahlreiche offene Fragen. Letztlich konnten diese auch nach Überarbeitung der Vertragsunterlagen von Microsoft nicht abschließend und zur Zufriedenheit der beteiligten Behörden beantwortet werden.

Kennzeichnend für eine Auftragsdatenverarbeitung in Form des Cloud-Computing ist es, dass der Auftraggeber – hier also die niedersächsische Behörde – für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich bleibt, also insbesondere für die Zulässigkeitsvoraussetzungen einer Datenverarbeitung und die Betroffenenrechte. Ferner wird der Auftragnehmer – hier also der Datentreuhänder – nur als unterstützendes Werkzeug in völliger Weisungsabhängigkeit für den Auftraggeber tätig. Die individuelle und undurchsichtige Vertragsausgestaltung in Form mehrerer vorformulierter Verträge erwies sich aus Sicht des Datenschutzes als bedenklich. Die Regelungen waren mit Blick auf die Auftragsdatenverarbeitung nicht eindeutig. Insbesondere blieb die rechtliche Position des Datentreuhänders als Auftragnehmer im Unklaren. Zwar wird der Zugriff auf die Kundendaten und damit die Schlüsselgewalt über die Daten vertraglich zwischen Datentreuhänder (Auftragnehmer) und dem Kunden (Auftraggeber) geregelt. Es existiert jedoch darüber hinaus noch ein Vertrag zwischen dem Datentreuhänder und dem Betreiber des Rechenzentrums (Microsoft), der nicht einsehbar war und daher auch keiner datenschutzrechtlichen Prüfung unterzogen werden konnte. Damit bleibt das Risiko, dass amerikanische Behörden über dieses Einfallstor weiterhin Zugriff auf die Daten des Rechenzentrums erlangen können, zumal der Datentreuhänder im Konzern betrachtet auch über Tochterunternehmen mit Sitz in den USA verfügt.

Ferner sieht das Vertragswerk vor, dass Microsoft weitere Unterauftragsdatenverarbeiter ohne ausdrückliche Zustimmung des Auftraggebers einbinden darf. Unter diesen Umständen ist eine gesetzlich vorgeschriebene sorgfältige Auswahl geeigneter Auftragnehmer durch die verantwortliche Stelle nicht mehr gewährleistet.

Nutzung der Deutschland-Cloud nicht empfehlenswert

Weitere Unklarheiten ergaben sich für mich in Bezug auf Rechteübertragungen im Rahmen der sog. Online Services Terms (OST). Diese sollen notwendige Wartungsarbeiten im Rechenzentrum regeln. Es ist datenschutzrechtlich bedenklich, dass nach der Gewährung des Zugriffes für die Dauer einer Fernwartung keine ausreichende Überwachung der in deren Rahmen durchgeführten Arbeiten stattfindet. Hinzu kommt, dass diese Wartungsarbeiten von Mitarbeitern im weltweiten Microsoft-Konzern nach dem „Follow-the-sun"-Prinzip durchgeführt werden. Das bedeutet, dass je nach Tageszeit die Fernwartung auch aus Ländern erfolgen kann, in denen weder der Schutz der EU-Datenschutzrichtlinie noch der ohnehin fragwürdige Schutz des US-Privacy-Shields gilt, so z. B. in Indien.

Ferner fehlte im Vertragswerk eine explizite Verankerung der Einhaltung von Vorgaben des niedersächsischen Datenschutzgesetzes. Dies betraf insbesondere die gesetzlichen Regelungen zur Auftragsdatenverarbeitung aber auch zum technisch-organisatorischen Datenschutz.

Da bereits die rechtlichen Rahmenbedingungen nicht datenschutzkonform zu lösen waren, wurden die erforderlichen technischen und organisatorischen Maßnahmen für dieses Projekt nicht weiter geprüft.

Letztlich habe ich der von mir beratenen Behörde empfohlen, von einer Nutzung der sog. „Deutschland-Cloud" der Fa. Microsoft abzusehen. Dieser Empfehlung ist das MJ nach eigener behördeninterner Prüfung des Vertragswerks gefolgt.

2.4 Datenschutzrechtliche Aspekte des „Financial Blocking“ nach dem Glücksspielstaatsvertrag

Mit dem Glücksspielstaatsvertrag haben die Länder einen einheitlichen Rahmen zur Regelung des Glücksspiels geschaffen. Ziel ist die Verhinderung der Glücksspiel- und Wettsucht. Zu diesem Zwecke soll der natürliche Spieltrieb der Bevölkerung in geordnete und überwachte Bahnen gelenkt und der Ausbreitung von unerlaubten Glücksspielen in Schwarzmärkten entgegengewirkt werden. Wesentliches Element des Glücksspielstaatsvertrages ist das Totalverbot für Online-Glücksspiele (§ 4 Abs. 4 GlüStV). Mit einer Blockade des Zahlungsverkehrs soll illegales Glücksspiel unterbunden werden. Die Methode ist allerdings nicht fehlerfrei.

Das Financial Blocking ist in § 9 Abs. 1 Satz 3 Nr. 4 GlüStV geregelt. Demnach kann die Aufsichtsbehörde den am Zahlungsverkehr Beteiligten, insbesondere den Kredit- und Finanzdienstleistungsinstituten, die Mitwirkung an Ein- und Auszahlungen für unerlaubtes Glücksspiel untersagen. Mit dieser Blockade des Zahlungsverkehrs soll der Tatsache Rechnung getragen werden, dass die

Anbieter von illegalen Internetglücksspielen oftmals ihren Sitz im Ausland haben, was eine Durchsetzung von Untersagungsverfügungen erschwert.

Das Unabhängige Landeszentrum für Datenschutz des Landes Schleswig-Holstein (ULD) hat im Januar 2015 datenschutzrechtliche Bedenken gegen das Financial Blocking erhoben. Im Kern wurde festgestellt, dass aus dem Glücksspielstaatsvertrag keine umfassende Befugnis zur Datenverarbeitung abgeleitet werden kann, die eine effektive Durchsetzung des Financial Blocking ermöglicht.

Maßnahmen zur Zahlungsunterbindung bedenklich

Ich habe daraufhin mit dem für länderübergreifende Glücksspiele zentral zuständigen Niedersächsischen Ministerium für Inneres und Sport die relevanten datenschutzrechtlichen Aspekte erörtert. Das Ministerium hat mehrfach darauf hingewiesen, dass es nicht beabsichtige, ein bundesweit einheitliches Verfahren zur Zahlungsunterbrechung einzuführen. Lediglich in Einzelfällen soll dafür gesorgt werden, dass den Spielanbietern keine Zahlungsmittel für das Internetangebot zur Verfügung stehen. Nach den mir zum Ende des Berichtszeitraumes vorliegenden Informationen sind Maßnahmen zur Zahlungsunterbindung gegen einen im Ausland ansässigen Anbieter von Internet-Casinospielen geplant, gegen den bereits eine gerichtlich bestätigte vollziehbare Untersagungsverfügung vorliegt.
Ich habe dem Ministerium mitgeteilt, dass ich es aus datenschutzrechtlicher Sicht begrüße, dass die geplante Zahlungsunterbindung nicht die Auszahlung des Gewinns von der Bank an die Spieler erfassen soll, da dies eine datenschutzrechtlich problematische Lokalisation der Teilnehmerinnen und Teilnehmer bedeutet hätte. Gleichwohl halte ich aber auch die geplanten Maßnahmen zur Zahlungsunterbindung des Spieleinsatzes für bedenklich. Denn dieses Verfahren ist bereits dann unsicher, wenn ein Veranstalter neben unerlaubtem Glücksspiel auch legale Dienste anbietet. In diesem Fall wäre nicht auszuschließen, dass eine Zahlungsunterbindung den legalen Dienst betrifft und damit fehlerbehaftet ist. Die Rechte der Betroffenen können auch nicht durch eventuelle Einspruchsmöglichkeiten gewahrt werden. Denn das geplante Verfahren kann nicht ausschließen, dass einzelne Bürgerinnen und Bürger schuldlos zu Unrecht in den Verdacht der Teilnahme an unerlaubtem Glücksspiel geraten und sich selbst durch aktives Tun von diesem Verdacht befreien müssen.

Das Verfahren wird von mir weiterhin kritisch begleitet werden.

2.5 Datenerhebung bei Abfallentsorgung auf Wertstoffhöfen:

Abfallwirtschaft der Region Hannover folgt den Empfehlungen des Datenschutzes

Im Frühjahr 2016 erreichten mich zwei Eingaben, die darauf hinwiesen, dass auf den Wertstoffhöfen des Zweckverbands Abfallwirtschaft Region Hannover (aha) bei Abfallanlieferungen mit Fahrzeugen, die über keine der Region Hannover zugehörigen Kfz-Kennzeichen verfügen, von der aha das Ausfüllen einer besonderen Erklärung gefordert würde. In dem entsprechenden Formular habe die anliefernde Person eine Vielzahl personenbezogener Daten, insbesondere Namen und Wohnort, anzugeben.

Hintergrund für diese Erhebung war, anhand der Erklärungen prüfen zu können, ob tatsächlich nur Abfälle angeliefert werden, die in privaten Haushalten erzeugt wurden, die sich in der Region Hannover befinden und die Abfälle nicht aus Gewerbebetrieben stammen oder gar außerhalb der Region Hannover erzeugt wurden. Bei Verstößen gegen diese Vorgaben dienen die Angaben in der Erklärung dazu, ggf. Personen von der Anlieferung auszuschließen.

Aus dem Formular der Erklärung ließ sich die erhebende Stelle nicht deutlich erkennen und es gab keine ausreichenden Informationen zur Verarbeitung der erhobenen Daten, insbesondere nicht dazu, aufgrund welcher Rechtsgrundlage erhoben und wie lange die erhobenen Daten gespeichert werden.

Der aha habe ich empfohlen, aus Gründen der Datensparsamkeit von der generellen Anforderung der Erklärung bei allen anliefernden Personen mit regionsfremden Kennzeichen abzusehen und sich stattdessen durch die Vorlage des Personalausweises dieser Personen die Abfallherkunft aus der Region nachweisen zu lassen. Der Nachweis einer Adresse im Regionsgebiet reicht aus, um anzunehmen, dass die angelieferten Abfälle in der Region erzeugt wurden und somit angeliefert werden dürfen.

Die aha folgte meinem Vorschlag; in der Tagespresse wurde anschließend ein Artikel zur neuen Praxis der aha veröffentlicht, in dem auch angeführt wurde, dass die Änderung auf Intervention meiner Behörde erfolgt sei.

2.6 Richtlinie zur Förderung der politischen Jugendbildung: Sozialministerium fragt sensible Teilnehmerdaten ab

Ausgelöst durch eine Beschwerde hat meine Behörde im Berichtszeitraum die Richtlinie des Ministeriums für Soziales, Gesundheit und Gleichstellung (MS) vom 07.12.2015 über die Gewährung von Zuwendungen zur Förderung der politischen Jugendbildung datenschutzrechtlich überprüft.

Nach Ziffer 6.6. dieser Richtlinie ist der Bewilligungsbehörde im Rahmen des vereinfachten Verwendungsnachweises eine vollständige Liste der Teilnehmenden der geförderten Maßnahme vorzulegen. Zudem sind Angaben über die Adressatinnen und Adressaten der Einladungen, die nicht Mitglied in der Jugendorganisation des Veranstalters sind, beizufügen.

Ich habe dem MS mitgeteilt, dass die gewählte Formulierung in der Richtlinie nicht gewährleisten kann, dass keine Rückschlüsse auf die politische Ausrichtung einzelner Teilnehmerinnen und Teilnehmer der geförderten Maßnahme gezogen werden können. Ein Bedarf für eine generelle Übermittlung dieser besonders sensitiven Daten an die Bewilligungsbehörde im Rahmen des vereinfachten Verwendungsnachweises wird nicht gesehen. Vielmehr wird es für ausreichend erachtet, dass der Zuwendungsempfänger diese besonders schutzwürdigen Daten vor Ort für eventuelle anlassbezogene oder stichprobenhafte Kontrollen der Bewilligungsbehörde vorhält.

Ich habe das MS daher gebeten, die Richtlinie zeitnah dahingehend zu überarbeiten, dass nur Angaben über die Anzahl der Adressatinnen und Adressaten der Einladungen, die nicht Mitglied in der Jugendorganisation des Veranstalters sind, beizufügen sind. Bis zu einer entsprechenden Änderung ist durch eine datenschutzkonforme Praxis sicherzustellen, dass ausschließlich anonymisierte Daten übermittelt werden, die keine Rückschlüsse auf die politische Ausrichtung einzelner Personen zulassen.

Zum Ende des Berichtszeitraums hat das MS mitgeteilt, dass die Richtlinie in vorgenannten Sinne datenschutzkonform geändert werden soll.

2.7 Übermittlung von Flüchtlingsdaten durch öffentliche Stellen

Die verstärkte Zuwanderung von Flüchtlingen in die Bundesrepublik im zweiten Halbjahr 2015 löste zahlreiche Anfragen zur Zulässigkeit von Datenverarbeitungen aus.

Die Anfragen von öffentlichen Stellen konzentrierten sich zum einen darauf, ob öffentliche Stellen wie Erstaufnahmeeinrichtung, Ausländerstelle, Jobcenter und Sozialamt etc. untereinander personenbezogene Daten der Flüchtlinge übermitteln dürfen. Ich habe die öffentlichen Stellen dahingehend beraten, dass es für eine Datenübermittlung zwischen öffentlichen Stellen stets einer Rechtsgrundlage bedarf.

Meine Überprüfung hat ergeben, dass es für die Übermittlung von Daten von ausländischen Flüchtlingen mit unterschiedlichem Aufenthaltsstatus (z. B. Asylbewerber, Geduldete) bereits nach unterschiedlichen Rechtsgrundlagen (wie beispielsweise dem Ausländergesetz, Asylgesetz, Asylbewerberleistungsgesetz oder Ausländerzentralregistergesetz) Übermittlungsbefugnisse gibt, die einen Datenaustausch zwischen öffentlichen Stellen ermöglichen, soweit dieser zur Aufgabenwahrnehmung erforderlich ist.

Übermittlung an Vereine und Organisationen nur nach Einwilligung der Betroffenen

Ein weiterer Fragekomplex bezog sich darauf, ob öffentliche Stellen personenbezogene Daten von Flüchtlingen an nicht-öffentliche Stellen wie ehrenamtlich helfende Personen, Vereine, Hilfsorganisationen etc. übermitteln dürfen.

Für die Übermittlung an nicht-öffentliche Stellen bedarf es mangels einer Rechtsgrundlage einer Einwilligung der betroffenen Flüchtlinge. Damit eine Einwilligung datenschutzrechtlich Bestand haben kann, muss diese freiwillig und informiert erfolgen. Aufgrund der zumeist vorhandenen Sprachbarrieren stellt dies eine besondere Herausforderung dar. Wenn es sich für die Betroffenen um lebensnotwendige Maßnahmen, wie zum Beispiel die Unterbringung oder Versorgung mit Lebensmitteln gehandelt hat, halte ich es gegenüber nicht kommerziellen Helfern für akzeptabel, wenn die Betroffenen bestmöglich über Inhalt und Zweck der Maßnahme aufgeklärt werden.

Eine weitere Fragestellung erstreckte sich darauf, ob Betreuer nicht-öffentlicher Stellen wie Hilfsorganisationen oder ehrenamtliche Helfer wiederum selbst Daten von Flüchtlingen erheben und an öffentliche Stellen übermitteln dürfen. Hier gilt das Gleiche: entweder bedarf es der Einwilligung der betroffenen Flüchtlinge oder die Betreuer müssen im Auftrage der öffentlichen Stelle tätig sein.

Bei der Erstunterbringung der Flüchtlinge in Notunterkünften erfolgt die Erhebung von personenbezogenen Daten vielfach durch private Hilfsorganisationen für Zwecke der Essensversorgung, aber auch zur Übermittlung für die weitere Nutzung an öffentliche Stellen im Rahmen von Unterbringungsleistungen. In Gesprächen mit Wohlfahrtsverbänden habe ich darauf hingewiesen, dass es für derartige Datenverarbeitungen eines Vertrags zwischen der Einrichtung und dem Land Niedersachsen bedarf, da hier hoheitliche Aufgaben für das Land wahrgenommen werden.

Die anfragenden Stellen wurden von mir entsprechend beraten und werden die datenschutzrechtlichen Anforderungen umsetzen.

Nutzung privater Dienstleister nicht erforderlich

Neben den Behörden, Ehrenamtlichen und sonstigen Hilfseinrichtungen haben sich auch kommerzielle Anbieter Gedanken gemacht, wie diese die Flüchtlinge unterstützen können. Sehr schnell gab es verschiedene Angebote für Flüchtlinge auf dem Markt, von einer Gesundheitskarte bis hin zu einer Refugee-Identification-Card. Daten, welche ausschließlich in der Hoheit eines privaten Anbieters gespeichert werden, mögen zwar für den persönlichen Gebrauch der Flüchtlinge, über verschiedene Dokumente in elektronischer Form verfügen zu können, praktisch erscheinen, für die Nachweisführung gegenüber öffentlichen Stellen sind diese Daten jedoch mangels hinreichender Authentizität nicht zu verwenden.

In einer Petition wurde ich darauf aufmerksam gemacht, dass eine Kommune das Angebot eines privaten Anbieters von Gesundheitskarten, welcher eine Art privates Cloud-Speicher-System für Gesundheits- und Asyldaten anbietet, nutzt. Die Kommune hatte zahlreiche Karten gekauft, um sie den Flüchtlingen zur Verfügung zu stellen. Bei dem betroffenen Personenkreis wurde durch die Ausgabe und Finanzierung der Karten durch die Kommune der Anschein erweckt, dass es sich um eine verpflichtende, staatliche Karte handelt. Nach Schilderung meiner datenschutzrechtlichen Bedenken, ob bei dem Personenkreis eine freiwillige, informierte Einwilligung für eine rein privatrechtlich zu nutzende Karte vorliegen kann, hat die Kommune davon abgesehen, die Karte weiter einzusetzen.

Mit Abschluss der Rahmenvereinbarung der Landesregierung mit den Landesverbänden der gesetzlichen Krankenversicherung nach § 264 Abs. 1 SGB V zur Einführung der elektronischen Gesundheitskarte (eGK) für Asylsuchende vom 14.03.2016 haben die Landkreise und kreisfreien Städte seit dem 01.04.2016 die Möglichkeit dieser Vereinbarung beizutreten und so die Finanzierung der Gesundheitsversorgung der Flüchtlinge zu regeln. Die Inanspruchnahme privater Dienstleister ist daher nicht erforderlich.

2.8 Anforderungen durch das neue Bundesmeldegesetz: Anfragen und Beschwerden

Im Berichtszeitraum wurde das niedersächsische Meldegesetz (NMG) durch das Bundesmeldegesetz (BMG) zum 01.11.2015 abgelöst. In dieser Zeit erreichten mich zahlreiche Anfragen zum Melderecht. Dabei waren unterschiedliche Fallkonstellationen betroffen. Exemplarisch werden einige Konstellationen dargestellt:

Übermittlung von Meldedaten zu Zwecken der Wahlwerbung

Regelmäßig erhalten Wahlberechtigte vor Wahlen Werbematerialien von Parteien mit der Tagespost.
So erreichten mich auch im Zusammenhang mit der Niedersächsischen Kommunalwahl im September 2016 wieder zahlreiche Anfragen von wahlberechtigten Bürgerinnen und Bürgern, ob es zulässig sei, dass Parteien ihre Daten zum Zwecke der personalisierten Wahlwerbung von den Meldeämtern erhalten.
Ich habe die Petenten darüber beraten, dass eine Möglichkeit für die Übermittlung von personenbezogenen Meldedaten bestimmter Personengruppen an Kandidaten für politische Ämter und Parteien unter den Voraussetzungen des § 50 Abs. 1 Bundesmeldegesetz (BMG) besteht. Ich habe ebenfalls darüber informiert, dass § 50 Abs. 5 BMG die Möglichkeit eröffnet, der Datenweitergabe zu widersprechen und die meisten Meldeämter dafür bereits entsprechende Vordrucke zur Verfügung stellen. Auch habe ich den Petenten mitgeteilt, dass die Meldeämter aufgrund gesetzlicher Verpflichtung regelmäßig mit öffentlichen Bekanntmachungen (in der Regel über die Tagespresse) auf die Widerspruchsmöglichkeit hinweisen.
Aufgrund der zu jeder Wahl wiederkehrenden Anfragen habe ich schon vor einigen Jahren einen dauerhaften Beitrag auf meiner Homepage eingestellt. Daneben erfolgt rechtzeitig vor einer Wahl jeweils ein ergänzender auf die aktuell anstehende Wahl angepasster Beitrag auf der Startseite der Homepage.

Weiterhin erhielt ich eine Beschwerde von Eltern einer Erstklässlerin, die anlässlich der Einschulung des Kindes ein an dieses adressiertes Glückwunschschreiben eines Bürgermeisterkandidaten für die anstehende Kommunalwahl erhalten hatte. Die Eltern fragten mich, ob es zulässig sei, dass Meldedaten von Minderjährigen an Kandidaten für politische Ämter übermittelt werden.
Durch Nachfrage bei der zuständigen Gemeinde war allerdings festzustellen, dass das dortige Meldeamt den § 50 Abs. 1 S.1 BMG falsch ausgelegt hat, da nur Daten von Gruppen von Wahlberechtigten selbst herausgegeben werden dürfen, „soweit für deren Zusammensetzung das Lebensalter bestimmend ist“ (z. B. Erstwähler, Senioren), nicht jedoch von Wahlberechtigten, deren

Kinder mit einem bestimmten Lebensalter einer bestimmten Gruppe (hier: Einschulungskinder) zuzuordnen sind.
Die Gemeinde wurde auf die Unzulässigkeit der Datenübermittlung und die richtige Anwendung des BMG hingewiesen.

§ 50 Abs. 1 Bundesmeldegesetz (BMG)
Die Meldebehörde darf Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs der Wahl oder Abstimmung vorangehenden Monaten Auskunft aus dem Melderegister über die in § 44 Absatz 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Die Geburtsdaten der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Die Person oder Stelle, der die Daten übermittelt werden, darf diese nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten.

Übermittlung von Alters- und Jubiläumsdaten an Mandatsträger

In § 50 Abs. 2 des neuen BMG wurden die Regelungen zu Datenübermittlungen von Altersjubiläen von der Meldebehörde an Mandatsträger sowie Presse und Rundfunk geändert. Als Altersjubiläen sind somit nur der 70. Geburtstag und jeder fünfte weitere Geburtstag anzusehen. Erst ab dem 100. Geburtstag dürfen Meldedaten für jährliche Gratulationen an Mandatsträgern übermittelt oder an Organe der Gemeinde weitergegeben werden.
In 2016 erhielt ich die Anfrage, ob Meldedaten von Einwohnerinnen und Einwohnern, die einer bestimmten Altersgruppe angehören, an Mandatsträger oder Mitglieder des Ortsrats übermittelt werden dürfen, damit Senioren zur Weihnachtsfeier des Ortsrats oder ähnlichen Veranstaltungen eingeladen werden können.
Dem Petenten wurde mitgeteilt, dass § 50 Abs. 2 BMG keine Datenübermittlung an Mandatsträger zu dem Zweck, Einladungen zu Veranstaltungen zu verschicken, rechtfertigt. Ich habe auch darauf hingewiesen, dass eine Datenweitergabe nach § 37 BMG von der Meldebehörde an den Ortsrat (als Organ) ebenfalls nicht zulässig ist, da der Versand von derartigen Einladungen weder als öffentliche Aufgabe noch als erforderlich im Sinne des § 37 BMG anzusehen ist.

§ 50 Abs. 2 Bundesmeldegesetz (BMG)
Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde Auskunft erteilen über
1. Familienname,
2. Vornamen,
3. Doktorgrad,
4. Anschrift sowie
5. Datum und Art des Jubiläums.

Altersjubiläen im Sinne des Satzes 1 sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum.

Wohnungsgeberbestätigungen nach dem Bundesmeldegesetz

Um Scheinanmeldungen zu verhindern, sind Wohnungsgeber (z. B. Wohnungsverwalter) nunmehr gemäß § 19 Abs. 1 BMG verpflichtet, an der Anmeldung mitzuwirken, in dem sie der meldepflichtigen Person den Einzug schriftlich oder elektronisch bestätigen (Wohnungsgeberbestätigung).
Ist der Wohnungsgeber nicht gleichzeitig Eigentümer der Wohnung, umfasst diese Verpflichtung auch die Angabe des Eigentümers der Wohnung.
Ein Wohnungsverwalter, welcher auf den von einigen Gemeinden vorgegebenen Formularen für Wohnungsgeberbestätigungen den Namen und die Anschrift des Wohnungseigentümers angeben sollte, äußerte mir gegenüber Bedenken gegen diese Datenerhebung. Oftmals sei von der Person, die das Eigentum an der Wohnung hat, gerade nicht gewünscht, dass diese den Mietern namentlich bekannt sei, damit die Mieter sich ausschließlich an die beauftragte Wohnungsverwaltung (z. B. Immobilien-Service) wenden.
Dem Verwalter wurde die Zulässigkeit der Datenerhebung und dessen Zielrichtung erläutert. Die Erhebung der Eigentümerangabe ist gerade deswegen erforderlich, um dessen Auskunftsanspruch nach § 50 Abs. 4 bezüglich des Mieters zu gewährleisten.

§ 50 Abs. 4 Bundesmeldegesetz (BMG)
Die Meldebehörde hat dem Eigentümer der Wohnung und, wenn er nicht selbst Wohnungsgeber ist, auch dem Wohnungsgeber bei Glaubhaftmachung eines rechtlichen Interesses unentgeltlich Auskunft über Familiennamen und Vornamen sowie Doktorgrad der in seiner Wohnung gemeldeten Einwohner zu erteilen. Die Auskunft kann auf Antrag des Auskunftsberechtigten im elektronischen Verfahren erteilt werden; § 10 Absatz 2 und 3 gilt entsprechend.

2.9 Beratende Funktion im Niedersächsischen IT-Planungsrat:

Keine IT-Planungen ohne strategischen Datenschutz!

Der IT-Planungsrat Niedersachsen ist ein Gremium[1], das unter Vorsitz des IT-Bevollmächtigten der Landesregierung (CIO) im Niedersächsischen Ministerium für Inneres und Sport (MI) für die strategische Grundlage sorgt, um die Anforderungen, die aus dem IT-Planungsrat Bund/Länder auf das Land zukommen, bewältigen zu können. Vorrangig soll eine ausgereifte landesinterne Abstimmung ermöglicht werden, wenn Beschlussvorschläge auf Bund/Länder-Ebene herbeizuführen sind, insbesondere wenn die Angelegenheiten mehrerer niedersächsischer Ministerien (gem. § 22 der Gemeinsamen Geschäftsordnung der Landesregierung und der Ministerien in Niedersachsen - GGO) oder Interessen der Kommunen berührt sind. Aber auch eigene landesinterne strategische Planungen werden in diesem Gremium abgestimmt und die Verträglichkeit mit bundesweiten Absprachen sichergestellt.

Bereits in den bisherigen Tätigkeitsberichten seit 2009 wurden die Mitwirkungen und inhaltlichen Beratungshinweise meiner Behörde geschildert. Wie in den Vorjahren habe ich bei den Entscheidungen des Niedersächsischen IT-Planungsrates auch 2015 und 2016 durch den zuständigen Technikreferatsleiter wieder regelmäßig beratend mitgewirkt. Dies geschah und geschieht zu einem erheblichen Teil mit Blick auf die technisch-organisatorischen Aspekte, aber auch auf die materiellrechtlichen Beurteilungen der Standardisierung von IT und der Implementierung von IT-Verfahren (Prozesse) und IT-Infrastrukturen in der Landesverwaltung.

Im Berichtszeitraum sind aus der Sicht des Datenschutzes Themen herauszuheben, die sich mit der Telekommunikations-Infrastruktur, dem Projekt „e-Akte“ und der Verschlüsselung befasst haben.

Elektronische Aktenführung (Projekt e-Akte): Geändertes Konzept birgt Gefahren

Bereits in meinem vorigen Tätigkeitsbericht habe ich ausführlich vor dem Einsatz proprietärer und nicht standardkonformer Lösungen gewarnt, dennoch ist Microsofts Sharepoint die Basis des inzwischen in der Landesverwaltung eingeführten Dokumentenmanagementsystems, also der elektronischen Aktenführung namens „e-Akte“ geworden.

1 Die Landesregierung hat die Einrichtung eines Niedersächsischen IT-Planungsrates zum 1. April 2010 beschlossen.

Während von Gegnern freier Software oftmals mit den vermeintlich höheren Gesamtkosten (Total Cost of Onwership, TCO) argumentiert wird, freie Programme seien zwar in der Anschaffung kostenlos, aber dieser Vorteil würde doch höhere Kosten für Betrieb und Pflege (im Vergleich zu kommerziellen Programmen) mehr als aufgezehrt, war ein wesentliches Argument für die Auswahl von Sharepoint, dass die mit der Fa. Microsoft geschlossenen Lizenzabkommen die Nutzungsrechte für dieses Produkt bereits miteinschlössen.

Die enge Verflechtung Sharepoints mit den bereits im Einsatz befindlichen MS-Produkten Windows, Office und Exchange auf der Basis proprietärer Techniken erhöht die Herstellerabhängigkeit erheblich und stellt damit auch ein potentielles Verfügbarkeitsproblem dar; entsprechende negative Erfahrungen mit Bürokommunikationssystemen hat man in der Ministerialverwaltung bereits in der Vergangenheit machen müssen.

Ende-zu-Ende-Verschlüsselung fehlt immer noch

Eine Ende-zu-Ende-Verschlüsselung, wie ich sie bereits in meinem vorigen Tätigkeitsbericht gefordert habe, fehlt nach wie vor, trotz der gewachsenen Erkenntnisse über – auch staatliche – Angriffe auf die IT-Infrastrukturen (s. meine Hinweise im Artikel zum Niedersachsenclient zu Cyberattacken).

Bereits innerhalb des Landesnetzes sollten spätestens Daten ab der Schutzstufe D schon aus diesem Grunde nur Ende-zu-Ende-verschlüsselt versandt werden, weil regelmäßig wiederkehrend (wenngleich auch mit geringem Anteil) durch Bedienfehler oder mangelnde Achtsamkeit Daten an falsche Empfänger versandt werden; in diesem Falle würde die Verschlüsselung eine unbefugte Kenntnisnahme ausschließen.

Beim Versand von Personendaten müsste die Ende-zu-Ende-Verschlüsselung ohnehin Standard sein, denn die Einwilligung des Betroffenen legitimiert regelmäßig nur den Verarbeitungszweck, nicht aber jedoch unzureichende technisch-organisatorische Maßnahmen, über die der Betroffene im Regelfall ohnehin keine Kenntnis erlangen kann; insofern wäre auch eine Einwilligung in die unverschlüsselte Übersendung nicht vom Niedersächsischen Datenschutzgesetz (NDSG) und ergänzenden Datenschutzvorschriften abgedeckt.
Die Einführung einer wirksamen Ende-zu-Ende-Verschlüsselung würde das ohnehin kritisch zu bewertende Konzept des Einsatzes von Virenscannern auf Firewalls ebenso aushebeln, wie auch das zentrale Scannen auf dem Mailserver; hier bedarf es dringend einer Fortentwicklung der Sicherheitsarchitektur (s. Beitrag zum NIC Niedersachsenclient).

2.10 Niedersachsen-Client – der Standardarbeitsplatzrechner in der Landesverwaltung: Eine Fortschreibung

Mit der unter Zeitdruck durchgeführten Migration der Arbeitsplatzrechner auf Windows 8.1 (vergl. mein Tätigkeitsbericht 2013-2014, S. 172 ff.) sind einige Probleme des technisch-organisatorischen Datenschutzes gelöst worden, etliche bestehen geblieben und sogar neue hinzugekommen. Aufgrund der fortschreitenden technischen Entwicklung haben sich zudem neue Risiken ergeben, die eine große Herausforderung für den sicheren und datenschutzkonformen IT-Betrieb darstellen.

Die im o. g. Bericht dargestellten Probleme der Bedrohung aus dem Internet, der Sicherheitslücken auch in „Sicherheitsprodukten" wie den Virenscannern haben inzwischen sogar zugenommen, während geforderte konzeptionelle Verbesserungen des technischen Datenschutzes in Form der Virtualisierung und der Bildung von Sicherheitsdomänen nicht realisiert wurden.

Virenscanner

Bereits in meinem vorigen Tätigkeitsbericht habe ich darauf aufmerksam gemacht, dass Virenscanner nur von beschränktem Nutzen für die IT-Sicherheit sind. Dem seinerzeit berichteten Mangel an aktuellen Signaturen zur Erkennung bereits bekannter Schadprogramme versuchen die Hersteller zunehmend durch den Einsatz von Heuristiken zu begegnen. Auf diesem Weg wird versucht, auch unbekannten Schadcode durch Analyse seines Verhaltens bei der Ausführung in einer abgesicherten Umgebung innerhalb des Virenscanners zu begegnen.

Problem hierbei ist, dass diese Analysefunktionen selbst aus hochkomplexem und damit potentiell fehleranfälligem Programmcode bestehen; verbunden mit den weitreichenden Rechten, mit denen der Virenscanner im System versehen ist, ist ein erfolgreicher Angriff gegen den Virenscanner selbst wahrscheinlicher geworden und das Schadensniveau hoch[1].

Aus diesem Grund wird das Konzept des Virenscanners durch IT-Sicherheitsfachleute zunehmend in Frage gestellt[2]. Dennoch kommen Virenscanner weiter auf Arbeitsplatzrechnern ebenso zum Einsatz, wie auf Mail- und Dat-

1 vergl. http://www.syscan360.org/slides/2014_EN_BreakingAVSoftware_JoxeanKoret.pdf

2 vergl. https://funoverip.net/wp-content/uploads/2013/12/Turning-your-managed-AV-into-my-botnet_OWASP2013_Nokin-Jerome_v1.1.pdf

eiservern, wie auch Firewalls. Auf letzteren brechen sie zudem regelmäßig SSL-/TLS-verschlüsselte Verbindungen auf, um den eingehenden Datenstrom zu untersuchen.
Die Kritik der Fachleute geht inzwischen so weit, dass bereits zur Deinstallation von Virenscannern geraten wird[3]. Selbst Hersteller, die selbst Antivirenprogramme vertreiben, wie die Fa. Symantec, halten diesen Ansatz als Schutz vor Schadprogrammen für überholt[4].
Jüngst war auch der in Windows selbst integrierte Virenscanner von einer äußerst schweren Sicherheitslücke betroffen, die auf vielfältige Weise ausgenutzt werden konnte.

Ransomware

Im Berichtszeitraum hat die Bedrohung durch sog. Ransomware, also Verschlüsselungstrojaner, die die Datenbestände des Nutzers verschlüsseln und vorgeben, diese gegen Zahlung eines „Lösegeldes" wieder zu entschlüsseln, erheblich zugenommen. Derartige Angriffe werden verstärkt maßgeschneidert auf die potentiellen Opfer durchgeführt; auch Behörden in Niedersachsen sind Opfer entsprechender Angriffe geworden, die als Bewerbungsemail gestaltet waren.

Sicherheitsdomänen und Virtualisierung

Vor diesem Hintergrund ist der bereits durch mich im Rahmen der beratenden Projektbegleitung geforderte Einsatz von Virtualisierung für Programme, die nach draußen kommunizieren (vorrangig Webbrowser und Mailclient) und entsprechend Abschottungsmaßnahmen der Netzsegmente gegeneinander noch dringlicher geworden.

Eine Machbarkeitsstudie des ITN kommt zu dem Ergebnis: „Durch den Einsatz von Browser in the Box kann ein erhebliches Maß an Sicherheit für das Landesnetz gewonnen werden, ein Übersprung von Schadsoftware auf den Arbeitsplatzrechner des Nutzers wird - soweit technisch möglich - wirkungsvoll verhindert. […] Insgesamt bietet Browser in the Box ein sehr hohes Sicherheitsniveau und einen zuverlässigen Schutz vor Angriffen auf das innere Netz. Die Hürde für ein Durchbrechen der Sicherheitsmaßnahmen ist zwar theoretisch möglich, liegt aber außerordentlich hoch und ist in der Praxis nicht relevant."

Daher nehme ich mit Bedauern zur Kenntnis, dass von einem Einsatz von „Browser in the Box" in der Praxis dennoch abgesehen wird, weil der Anwender überfordert sei, die verbleibenden Restrisiken bei der Nutzung verantwortlich abzuschätzen: „Als sehr problematisch wird die Wahrnehmung der Benutzer gesehen, durch die Verwendung von Browser in the Box umfänglich geschützt zu sein."

3 siehe https://www.heise.de/security/artikel/Ex-Firefox-Entwickler-raet-zur-De-Installation-von-AV-Software-3609009.html

4 siehe https://www.heise.de/security/meldung/Symantec-erklaert-Antivirus-Software-fuer-tot-2183311.html

Aufgrund der beschriebenen Sicherheitsprobleme[5], ist die kleinteiligere Unterteilung der vorhandenen Netze in verschiedene Sicherheitsdomänen geboten, um zumindest den Umfang erfolgreicher Angriffe besser begrenzen zu können.

Diese Vorgehensweise ist zudem angeraten, da der Niedersachsenclient lediglich für die Verarbeitung von Daten der Schutzstufe C freigegeben ist und daher für die Verarbeitung von Daten mit höherem Schutzbedarf (z. B. in der Personalverwaltung) ergänzende Schutzmaßnahmen erforderlich sind.

Polizeiclient

Vor dem Hintergrund der beschriebenen Bedrohungen und auch künftig zu erwartenden Angriffen stellt die zunehmende technische Monokultur in der Landesverwaltung durch Umstellung der Polizeiarbeitsplätze von Linux auf eine Variante des Niedersachsenclients zumindest insofern ein zusätzliches Risiko dar, als das Schadensrisiko im Falle erfolgreicher Angriffe auf die Landesverwaltung steigt, wenn an einer steigenden Zahl von Arbeitsplätzen identische Technik zum Einsatz kommt.
In Anbetracht der geringen Verbreitung von Linux am Arbeitsplatz im Verhältnis auf den Gesamtmarkt stellt der Einsatz von Linux bereits dadurch ein Sicherheitsgewinn dar, weil die Wahrscheinlichkeit erfolgreicher Angriffe selbst dann abnimmt, wenn die effektive Sicherheit der Linux-Systeme nicht höher als die von vergleichbaren Windows-Systemen ist, weil eine Entwicklung von nicht zielgerichteten Schadprogrammen für Linux weniger gewinnversprechend ist.

Microsoft verschlechtert Datenschutz weiter

Mit der Ankündigung Microsofts[6], Rechner mit aktuellen Prozessoren nicht mehr mit Aktualisierungen für Windows 8.1 zu versorgen, wird sich die Landesverwaltung frühzeitig mit dem Problem konfrontiert sehen, bei den neu zu beschaffenden Rechnern Windows 10 einsetzen zu müssen, um arbeitsfähig zu bleiben. Hier aber hat die französische Datenschutzaufsichtsbehörde CNIL in einer Prüfung festgestellt, dass dieses Produkt mit europäischem Datenschutzrecht nicht vereinbar ist.

5 Anmerkung nach Redaktionsschluss: Auch die jüngste Cyberattacke mit der „WannaCry"-Ransomware, die in Großbritannien ganze Netzwerke lahmgelegt hat, hat diese Erkenntnis deutlich unterstrichen.

6 Siehe https://www.heise.de/newsticker/meldung/Windows-7-und-8-1-Keine-Windows-Updates-mit-neuen-Prozessoren-3656807.html

2.11 Aufsichtsbehördliche Zusammenarbeit der Dataport-Trägerländer

Dataport ist ein gemeinsames Rechenzentrum, das Rechenleistungen für die Bundesländer Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Sachsen-Anhalt und Schleswig-Holstein erbringt und in der Form einer Anstalt öffentlichen Rechts geführt wird.
Während Dataport für die Länder Bremen, Hamburg, Schleswig-Holstein wesentliche Teile der jeweiligen Landes-IT betreibt, beschränkt sich die Tätigkeit Dataports für die Länder Mecklenburg-Vorpommern und Niedersachsen auf Rechenzentrumsdienstleistungen für die Steuerverwaltung; daneben ist Dataport für viele schleswig-holsteinische Kommunalverwaltungen tätig.

Um die gemeinsame datenschutzrechtliche Zusammenarbeit der Aufsichtsbehörden zu gewährleisten, kommen die Behörden im halbjährlichen Turnus in Hamburg zur Beratung zusammen. Daneben dient dieses Gremium dem Austausch über datenschutzrechtliche und technisch-organisatorische Fragestellungen, die die Trägerländer gemeinsam tangieren. Hierzu gehören beispielsweise die Planungen für den gemeinsamen Betrieb eines Telekommunikationsüberwachungssystems (s. Artikel in diesem Tätigkeitsbericht Seite 32), oder ein bundesländerübergreifendes Verfahren zur Verkehrsflusserhebung und -steuerung im Rahmen der Bauarbeiten entlang der Autobahn A 7 im Hamburger Raum anhand von Bluetooth-Daten.

Länderübergreifende gebündelte Verfahrensbetreuung (LGVB)

Aufgrund steigender Einsparungsanforderungen an die Bundesländer wird die Zusammenarbeit im Bereich der Fachverfahren für die Finanzverwaltung intensiviert. Hierzu gehört, dass für diese Verfahren die Betreuung zentral nur von einem Bundesland für alle Mitgliedsländer erbracht wird; Grundlage für diese Form der Zusammenarbeit ist ein Staatsvertrag zwischen den beteiligten Ländern. Bei der Umsetzung gilt es auch, die datenschutzrechtlichen Anforderungen korrekt umzusetzen.

Mit diesem neuen Ansatz geht die Notwendigkeit einher, eine Reihe organisatorischer, technischer und rechtlicher Weichenstellungen für die Zusammenarbeit der beteiligten Länder vornehmen zu müssen. Prototypisch wurde dies bei der Einführung eines neuen IT-Verfahrens zu Stundung und Erlass („StundE") in Form einer Auftragsdatenverarbeitung umgesetzt.

Grundsätzlich werden die rechtlichen Anforderungen durch eine zeitgleich mit dem Staatsvertrag abgeschlossene Rahmenvereinbarung geregelt, in der

die datenschutzrechtlichen Grundlagen für die im Rahmen der LGVB einzuführenden IT-Verfahren festgelegt werden. Daneben werden für jedes einzelne Verfahren gesonderte gemeinsame Verabredungen getroffen, die in Form standardisierter Leistungsscheine festgelegt wurden.

Mandantentrennung

Wesentlichen Raum innerhalb des Berichtszeitraums hat die Beratung über die Gewährleistung der Mandantentrennung im Rahmen der Fortentwicklung der IT-Infrastruktur von Dataport eingenommen. Dabei muss jedes Land als ein separater Mandant bei Dataport gesehen werden. Dementsprechend gilt dies auch für die Verarbeitung der personenbezogenen Daten.

Da Dataport und seine Trägerländer im Wesentlichen auf Produkte aus dem Hause Microsoft setzen, beziehen sich die Probleme der Mandantentrennung vorrangig auf den Verzeichnisdienst „Active Directory (ADS)“, sowie die Einrichtung eines zentralen Serververbundes für E-Mail und Terminplanung („Community Cloud Mail System“, CCMS).

Einerseits besteht gerade bei den Hauptträgerländern der Bedarf, die Produkte Exchange/Outlook nicht nur für den Nachrichtenversand, sondern auch zur Terminvereinbarung und Ressourcenplanung länderübergreifend nutzen zu können, andererseits gilt es den Anforderungen der Mandantentrennung Rechnung zu tragen und personenbezogene Daten der Beschäftigten vor unbefugter Kenntnisnahme zu schützen.

Auch wenn Niedersachsen bedingt durch seine auf den Finanzbereich beschränkte Nutzung von Dataportdienstleistungen nicht betroffen ist, ist meine Behörde in vergleichbarer Weise mit dieser Fragestellung bei der rechtlichen Bewertung des IT-Betriebes beim Landesbetrieb IT-Niedersachsen konfrontiert, der für eine Vielzahl von Landesdienststellen Dienstleistungen erbringt. Letztlich hat die Erörterung ergeben, dass der Datenaustausch aufgrund der Erforderlichkeit für die Aufgabenerfüllung der angeschlossenen Länder zulässig ist.

2.12 IT-Strategie der Landes Niedersachsen „Digitale Verwaltung 2025“

Die Landesregierung hat in ihrer Sitzung am 27.09.2016 die IT-Strategie des Landes Niedersachsen mit dem Titel „Digitale Verwaltung 2025“ beschlossen. Sie stellt einen Orientierungs- und Handlungsrahmen für die Entwicklung der IT der Landesverwaltung vor dem Hintergrund der Digitalisierung der Gesellschaft dar. Zu diesem Zweck wurde die IT-Gesamtstrategie für die Landesverwaltung aus dem Jahr 2012 entsprechend dem Kabinettsauftrag aus dem Jahr 2013 unter Beteiligung des Niedersächsischen IT-Planungsrats aktualisiert und weiterentwickelt. Grundlage der Ressortbeteiligung war ein überarbeiteter Entwurf vom 09.09.2015. Zu diesem Entwurf habe auch ich umfassend Stellung genommen.

In der verabschiedeten Fassung sind weite Teile des Entwurfs neu gefasst worden. Während meinen Hinweisen und Anregungen an vielen Stellen gefolgt wurde, sind jedoch Einzelaussagen des ursprünglichen Entwurfes zu Gunsten zusammenfassender Gesamtdarstellungen aufgegeben worden, was im Ergebnis zu weniger konkreten Aussagen in wichtigen Themenfeldern führt. So bleibt z.B. unklar, inwieweit die Landesregierung meiner Betonung des Primats des Datenschutzes gegenüber den Anforderungen der Haushaltssparsamkeit oder den Begehrlichkeiten weitergehender Datennutzungen zu folgen bereit ist. Auch wurde meiner dringenden Empfehlung, einen Katalog von Vertraulichkeitskriterien – sowohl für die Auswahl von Hardware-, Software- und Netzprodukten als auch für die Auswahl von Dienstleistungprodukten bei der Zusammenarbeit mit Herstellern und Dienstleistern – zu erarbeiten, leider nicht gefolgt.

Dennoch beschreibt die vorliegende Fassung die Herausforderungen der Digitalisierung sowohl für den Staat und seine Verwaltung wie auch für die Gesellschaft als Ganzes im Wesentlichen zutreffend; auch die Darstellung der allgemeinen politischen Rahmenbedingungen stellt eine Reihe von Aspekten für die Fortentwicklung der öffentlichen IT-Landschaft in Niedersachsen nachvollziehbar dar und erteilt der unkritischen Privatisierung von IT-Leistungen für die öffentliche Verwaltung eine klare Absage.

Datenschutz zwischen Standardisierungsbemühungen und wirtschaftlichen Interessen

Im Themenfeld „Innovative Verwaltung“ werden verschiedene Aspekte des elektronischen Verwaltungshandelns betrachtet, und im Kern wird eine verbesserte Interoperabilität der Verwaltungsbereiche angestrebt. Obwohl dieser Aussage im Grundsatz zugestimmt werden kann, gebe ich zu bedenken, dass diese verbesserte Interoperabilität keineswegs zu einer Beliebigkeit der Nut-

zung personenbezogener Daten innerhalb des öffentlichen Sektors führen darf. Die strikten Grenzen, die das Datenschutzrecht der Übermittlung und dem Austausch personenbezogener Daten setzt, sind durch geeignete technisch-organisatorische Maßnahmen sicher umzusetzen. Hinter dieser zwingenden Notwendigkeit müssen Fragen der Interoperabilität und Wirtschaftlichkeit im Zweifel zurücktreten.

Die im Themenfeld „Ebenen- und länderübergreifende Zusammenarbeit" angestrebte Standardisierung von IT-Ressourcen und Sicherheitsniveaus wird von mir ausdrücklich begrüßt. Ich gebe allerdings zu bedenken, dass die Standardisierungsbemühungen nicht zu einem Verzicht auf eigene Datenschutz- und Sicherheitsanforderungen auf Seiten der jeweiligen Nutzer führen dürfen.
Auch muss in geeigneter Weise Vorsorge getroffen werden, dass die Zentralisierung von IT-Ressourcen nicht mit Risiken für die Verfügbarkeit der Daten, Systeme und Prozesse einhergeht , die im Extremfall zu einem Totalausfall einer Gesamtinfrastruktur, eines Gesamtverfahrens oder sogar aller angeschlossenen Verwaltungseinheiten führen könnte[1]. Ebenso ist sicher zu stellen, dass bei der gemeinsamen Nutzung von Ressourcen der Grundsatz der Zweckbindung sowie die Nichtverkettbarkeit verarbeiteter personenbezogener Daten stets eingehalten wird. Hier bleibt die konkrete Ausgestaltung abzuwarten.

Die im abschließenden „Ausblick" getroffene Aussage, dass es zwingend notwendig sei, künftig vermehrt in die Modernisierung der IT-Infrastruktur der Landesverwaltung zu investieren, kann von meiner Seite nur unterstrichen werden. Ich möchte an dieser Stelle aber noch einmal darauf hinweisen, dass eine möglichst wirtschaftliche Neuorganisation nicht zu Abstrichen bei der Umsetzung der datenschutzrechtlich gebotenen technisch-organisatorischen Maßnahmen führen darf.

1 Dieser Effekt wird als die Gefahr eines „Single Point of Failure" bezeichnet, also der Gefährdung der Verfügbarkeit im Fall, dass der Ausfall eines einzigen kritischen Bestandteils eines Gesamtsystems den Ausfall des gesamten Systems verursacht.

3. Schulen

3.1 Einsatz von Online-Lernplattformen im Schulunterricht

Immer mehr Bildungsinstitutionen setzen auf eine webgestützte Wissensvermittlung und auf elektronische Kommunikationsmöglichkeiten zwischen Lehrenden und Lernenden. Hierfür sind klar umrissene Regeln erforderlich.

Bereits im Tätigkeitsbericht 2013-2014 habe ich im Beitrag „Webbasierte Lernplattformen und Whiteboards“ ausgeführt, dass einheitliche und eindeutige Rahmenbedingungen für die Nutzung dieser Verfahren in den Schulen erforderlich sind.

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder hat am 08.04.2016 die „Orientierungshilfe für Online-Lernplattformen im Schulunterricht“ beschlossen. Diese richtet sich insbesondere an Schulen, die Online-Lernplattformen als Lernmittel einsetzen und beschreibt dafür die datenschutzrechtlichen Mindestanforderungen. Sie gibt zudem auch den Anbietern von Online-Lernplattformen die Möglichkeit, ihr jeweiliges Produkt so zu gestalten oder anzupassen, dass eine datenschutzkonforme Nutzung durch die Schulen zulässig ist.

Die Orientierungshilfe habe ich an das Niedersächsische Kultusministerium, die Niedersächsische Landesschulbehörde und das Niedersächsische Landesinstitut für schulische Qualitätsentwicklung mit der Bitte um Weiterleitung an die Schulen gegeben. Zudem ist sie auch auf meiner Homepage veröffentlicht[1].

1 https://www.lfd.niedersachsen.de/themen/schulen/datenschutz-in-schulen-56175.html

3.2 Einsatz von Tablets im Schulunterricht: Anforderungen an den Datenschutz

Der Einsatz von Tablets im Schulunterricht wird immer populärer. Er weist aber immer noch erhebliche datenschutzrechtliche Risiken auf, die nur durch geeignete Datenschutzkonzepte der Schulen als verantwortliche Stellen beherrscht werden könnten.

Bereits im Jahr 2012 hatte mein Vorgänger das Niedersächsische Kultusministerium gebeten, ein landesweites Datenschutzkonzept für die Tablet-Klassen zu entwickeln, um die Schulen entsprechend zu entlasten.

Im Berichtszeitraum wurde anlässlich von Eingaben jedoch erkennbar, dass die niedersächsischen Schulen immer noch keine Datenschutzkonzepte haben. Auf meine Anregung hat das Niedersächsische Landesinstitut für schulische Qualitätsentwicklung (NLQ) im Jahr 2016 den Entwurf eines Leitfadens zum Einsatz mobiler Computer im Unterricht vorgelegt. Dieser wurde in einer Besprechung mit dem Niedersächsischen Kultusministerium (MK), dem NLQ, der Niedersächsischen Landesschulbehörde, der Landesinitiative „n-21: Schulen in Niedersachsen online e. V." und meiner Behörde eingehend in datenschutzrechtlicher Hinsicht erörtert. Der Leitfaden wird gegenwärtig nach meinen Hinweisen weiterentwickelt. Nach Fertigstellung des Leitfadens wird den Schulen eine gute Grundlage zur Einhaltung des Datenschutzes bei Tablet-Klassen zur Verfügung stehen.

Aus meiner Sicht ist es dringend geboten, dass das MK diesen Leitfaden für alle Schulen für verbindlich erklärt.

3.3 Datenschutz in der Schule:

Einsatz privater IT-Systeme zur Erledigung dienstlicher Aufgaben

Lehrer können im Unterricht durchaus private IT-Geräte nutzen. Für deren datenschutzrechtlich akzeptablen Einsatz in der Schule sind allerdings strikte Voraussetzungen bei der Datenspeicherung einzuhalten.

Das Land stellt seinen Lehrkräften nicht durchgängig die zur Erledigung ihrer dienstlichen Aufgaben benötigten IT-Geräte zur Verfügung. Deswegen nutzen viele Lehrkräfte hierfür ihre eigenen Geräte. Dies wird unter dem Schlagwort „Bring your own device – BYOD" – zusammengefasst. Das Niedersächsische Kultusministerium (MK) hat in dem Runderlass vom 01.02.2012 „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Lehrkräften"[1] geregelt, unter welchen Voraussetzungen die Lehrkräfte ihre eigenen, privaten IT-Geräte einsetzen dürfen. Dieser Erlass differenziert noch nicht zwischen mobilen Endgeräten wie Smartphones und Tablet-PCs und „herkömmlichen" Desktop-PCs. Aus datenschutzrechtlicher Sicht müssen die Lehrkräfte die nach § 7 NDSG erforderlichen technisch-organisatorischen Maßnahmen sicherstellen. Dies bedeutet, dass die Geräte die Anforderungen an den Datenschutz erfüllen. Die Geräte müssen technisch auf dem gängigen Sicherheitsstandard gehalten werden und sind so zu konfigurieren, dass nur die zulässigen Daten verarbeitet werden können. Dies ist aber praktisch gar nicht möglich, da die auf diesen mobilen Endgeräten laufenden Betriebssysteme wie z. B. Android und iOS als prinzipiell unsichere Plattformen gelten. Sie senden oftmals im Hintergrund und ohne, dass der Nutzer davon etwas erfährt, sehr viele Nutzerdaten über das Mobilfunknetz. Dabei bieten sie zu wenige, unvollständige oder schlecht bedienbare Möglichkeiten, Einstellungen für den Datenschutz vorzunehmen. Damit kann schon eine der Grundvoraussetzungen des o.a. MK-Erlasses nicht erfüllt werden, nämlich dass nur die Lehrkraft selbst Zugang zu den Daten der Schülerinnen und Schüler erhält.

Ich habe das MK im Berichtszeitraum mehrfach darauf hingewiesen, dass eine dienstliche Bereitstellung von IT-Geräten für die Lehrkräfte die bessere Alternative darstellen würde. Dies ist aus Sicht des MK jedoch nicht finanzierbar. Meine Behörde erachtet die Nutzung privater mobiler IT-Geräte nur dann für hinnehmbar, wenn gewährleistet ist, dass das private Gerät lediglich als Web-Endgerät genutzt wird. Das bedeutet, dass die Datenspeicherung ausschließlich auf einem gesicherten Server der Schule stattfindet. Dabei muss zugleich ausgeschlossen werden, dass Daten aus dem System auf das mobile Gerät kopiert und dort zusätzlich lokal in einer App gespeichert werden können.
Ich habe das MK gebeten, den Erlass zeitnah durch Einfügung einer neuen Teilziffer bezüglich des Einsatzes mobiler Endgeräte in dem o. a. Sinne einzuschränken. Kurz nach Ablauf des Berichtszeitraums hat das Kultusministerium mitgeteilt, dass es den Erlass zeitnah anpassen wird.

1 http://www.nds-voris.de/jportal/?quelle=jlink&query=VVND-206000-MK-20120201-SF&psml=bsvorisprod.psml&max=true

3.4 Foto- und Filmaufnahmen in der Schule – immer nur mit Einwilligung!

Vermehrt wenden sich Firmen, die sich auf das Anfertigen von Klassenfotos oder Einzelfotos von Schülerinnen und Schülern spezialisiert haben an die Schulleitungen und bieten ihre Dienste an. Im Berichtszeitraum haben mich einige Anfragen erreicht, die sich auf die Anfertigung von Fotos von Schülerinnen und Schülern in der Schule und die Veröffentlichung von Fotos auf der Schul-Website beziehen.

Ich habe die Petenten und die Schulleitungen stets darauf hingewiesen, dass es nicht zu den Aufgaben der Schule gehört, Fotos anfertigen zu lassen und diese ggf. zu veröffentlichen. Mangels einer Rechtsgrundlage ist das Fotografieren der Schülerinnen und Schüler und das Übermitteln ihrer Daten, wie beispielsweise Name, Anschrift und Geburtsdatum, an einen externen Dienstleister nur dann zulässig, wenn die Erziehungsberechtigten eingewilligt haben. Haben die Schülerinnen und Schüler das 15. Lebensjahr vollendet, muss neben der Einwilligung der Erziehungsberechtigten auch die der Minderjährigen selbst eingeholt werden.

Entsprechendes gilt für die Frage der Veröffentlichung von Fotos auf der Schul-Website sowie von Filmen. Auch insoweit bedarf es einer Einwilligung der Betroffenen. Dabei sind die Zwecke, zu denen die Veröffentlichung erfolgen soll, so präzise wie möglich zu benennen (z. B. Sportfest, Weihnachtsfeier). Finden einmalige Ereignisse (z.B. Jugend forscht) statt, empfiehlt es sich, im Zusammenhang mit der Teilnahmeabfrage bei den Eltern auch gleichzeitig eine Einverständniserklärung zur Veröffentlichung von Fotos oder Filmen einzuholen.

3.5 Kommunales Bildungsmonitoring: Schulen dürfen nur Daten ohne Personenbezug an die Bildungsregionen herausgeben

Dank einer rechtzeitigen Anfrage an meine Behörde konnte ich eine Bildungsregion beim Aufbau eines datenschutzkonformen Bildungsmonitorings beraten. Insbesondere Datenschutzverstöße aufgrund einer unzulässigen Übermittlung personenbezogener Daten konnten so vermieden werden.

Das Niedersächsische Kultusministerium (MK) hat im Juni 2015 ein „Rahmenkonzept für Bildungsregionen in Niedersachsen" herausgegeben. Darin empfiehlt es den den Akteuren die sich im Bildungsbereich zu einer sogenannten Bildungsregion, vernetzten, ein kommunales Bildungsmonitoring aufzubauen, um auf datenbasierter Grundlage die bildungsregionale Entwicklung steuern und Entscheidungen begründen zu können.

In diesem Zusammenhang ist eine Bildungsregion an mich herangetreten und hat mir ihr Konzept zum Aufbau eines Bildungsmonitorings vorgelegt. Ziel war es, einen Bildungsbericht zu erstellen, der den Entwicklungsstand der Region erfasst. Dazu sollten die Schulen der Region personenbezogene Daten der Schülerinnen und Schüler (u. a. Postleitzahl, Wohnort, Straße, Hausnummer) an den Landkreis als Schulträger übermitteln, der diese sammelt und an die mit der Bildungsberichterstellung beauftragte Stelle weiterleiten sollte.

Da eine Einwilligung der Betroffenen in die vorgesehene Datenübermittlung nicht vorlag, wäre diese Datenübermittlung personenbezogener Daten nur zulässig gewesen, wenn sie sich auf eine Rechtsgrundlage hätte stützen können.

Die Bildungsregion ist davon ausgegangen, dass § 31 Abs. 1 Satz 1 Niedersächsisches Schulgesetz (NSchG) als Rechtsgrundlage in Betracht kommt. Demnach dürfen Schulen, Schulbehörden, Schulträger, Schülervertretungen und Elternvertretungen personenbezogene Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten (§ 55 Abs. 1) verarbeiten, soweit dies u. a. zur Erforschung oder Entwicklung der Schulqualität erforderlich ist.

Da die Erforschung und Entwicklung der Schulqualität immer in Bezug auf die einzelne Schule zu sehen ist, hier aber eine regionale Auswertung der Bildungschancen erfolgen sollte, und diese zudem nicht zu dem Aufgabenbereich der Schulträger gehört, konnte die Übermittlung personenbezogener Daten nicht auf § 31 Abs. 1 NSchG gestützt werden. Eine andere Rechtsgrundlage für die Übermittlung personenbezogener Daten der Schülerinnen und Schüler kam nicht in Betracht, so dass ich der Bildungsregion vorgeschlagen habe, den Datentransfer in der Weise vorzunehmen, dass kein Personenbezug herstellbar ist. Konkret könnte der Transfer erfolgen, wenn die Angaben zu Postleitzahl, Wohnort, Straße und Hausnummer der Schülerinnen und Schüler unterbleiben würden, so dass keine Rückschlüsse auf einzelne Schülerinnen und Schüler möglich sind. Das MK hat sich meiner Auffassung angeschlossen. Ich habe die Bildungsregion entsprechend informiert.

3.6 Datenschutz in schulischen Gremien

Immer wieder erreichen mich Fragen zum Datenschutz in Schulen und deren Gremien. Bespielhaft werden an dieser Stelle zwei dieser Fragen vorgestellt.

Ein Vorsitzender einer Klassenelternschaft erkundigte sich, ob die Schule die Übermittlung der für die Kommunikation mit der Elternschaft benötigten Kontaktdaten der Eltern der Schülerinnen und Schüler verweigern könne. Gegen eine Datenübermittlung bestehen insoweit keine Bedenken. Die Beteiligung der Erziehungsberechtigten an schulischen Entscheidungen erfolgt nach § 88 Abs. 1 Nr. 1 Niedersächsisches Schulgesetz (NSchG) u.a. durch die Klassenelternschaft und wird in den Elternversammlungen realisiert. Für die Einladungen zu den Elternversammlungen ist die Erhebung der Kontaktdaten der Erziehungsberechtigten bei der Schule erforderlich.

In einem anderen Fall erkundigte sich eine Lehrkraft, ob sie Einsicht in die Protokolle des Schulelternrats nehmen darf. Es gab Befürchtungen, dass wegen vorhandener Konflikte zwischen Eltern und einzelnen Lehrkräften dort Daten zu ihrer Person erfasst worden seien. Der Lehrkraft wurde mitgeteilt, dass sie gemäß § 16 Abs. 1 Niedersächsisches Datenschutzgesetz (NDSG) ein Auskunftsrecht bzw. Einsichtsrecht in die Protokolle des Schulelternrates bezüglich der zu ihrer Person gespeicherten Daten hat. Diese Auskunft darf sich allerdings ausschließlich auf die Passagen beschränken, in denen personenbezogenen Daten dieser Lehrkraft verarbeitet worden sind. Daten anderer Personen, die dort erwähnt werden, müssen unkenntlich gemacht werden.

4. Gesundheit und Soziales

4.1 „Klinisches Krebsregister Niedersachsen“: Recht auf informationelle Selbstbestimmung der Betroffenen muss gewahrt bleiben

Bereits im letzten Tätigkeitsbericht habe ich unter dem Punkt „Krebsregistrierung in Niedersachsen – Meldepflicht und Datenschutz austariert“ erwähnt, dass die Länder aufgrund des am 03.04.2013 beschlossenen Krebsfrüherkennungs- und -registergesetzes aufgefordert sind, behandlungsbezogene klinische Krebsregister zu errichten und die rechtlichen Grundlagen hierfür zu schaffen.

Im Berichtszeitraum wurde durch das Ministerium für Soziales, Gesundheit und Gleichstellung (MS) der Entwurf eines Gesetzes über das klinische Krebsregister in Niedersachsen (GKKN) erarbeitet. Zu verschiedenen Kernfragen des Datenschutzes habe ich an der Arbeitsgruppe des MS teilgenommen, um sicherzustellen, dass das Recht auf informationelle Selbstbestimmung der Betroffenen einen hohen Stellenwert im GKKN erhält.

Zum Ende des Berichtszeitraums wurde mir ein erster Vorentwurf des GKKN zur datenschutzrechtlichen Prüfung vorgelegt. Ich werde bei der weiteren Begleitung des Gesetzgebungsverfahrens darauf hinwirken, dass dem Recht auf informationelle Selbstbestimmung der Betroffenen umfassend Rechnung getragen und bereits durch entsprechende Regelungen im Gesetz umfassend geschützt wird.
Aus meiner Sicht sind unter anderem das Widerspruchs- sowie das Auskunftsrecht der Betroffenen wesentliche Punkte. Gerade in einem Gesetz, welches den Umgang mit den sensibelsten Daten eines Menschen, die Tatsache einer Krebserkrankung, regelt, muss den Betroffenen das Recht zugestanden werden, eine Verarbeitung personenbezogener Daten ablehnen zu können. Aus diesem Grund lege ich sehr viel Wert auf eine umfassende Widerspruchsmöglichkeit der Betroffenen.

Neben der rechtlichen Arbeit im Gesetzgebungsverfahren hat auch eine Arbeitsgruppe des zukünftigen Klinischen Krebsregisters die Planung und Ausar-

beitung der technisch-organisatorischen Voraussetzungen begonnen. Damit Recht und Technik datenschutzrechtlich Hand in Hand gehen, habe ich auch dieser Arbeitsgruppe beratend zur Seite gestanden.

Hierzu fand Mitte 2016 ein erstes Treffen zu den Themenfeldern Softwarekomponenten, Netzwerkarchitektur und Datenverarbeitung statt, in dem die geplante IT-Infrastruktur vorgestellt und damit einhergehende Problemfelder erörtert wurden. Darüber hinaus wurde abgestimmt, wie meine Behörde dieses Projekt in Zukunft begleiten könnte. Von einem intensiven Austausch zu Fragen und Problemstellungen des materiell rechtlichen und technisch-organisatorischen Datenschutzes versprechen sich sowohl die Projektgruppe als auch ich eine win-win-Lösung im Interesse der Betroffenen.

4.2 Gesundheitsregionen in Niedersachsen werden datenschutzrechtlich geprüft

Zur Unterstützung der Landkreise und kreisfreien Städte bei der Gestaltung des regionalen Gesundheitswesens hat die niedersächsische Landesregierung gemeinsam mit verschiedenen Partnern das Projekt „Gesundheitsregionen in Niedersachsen" ins Leben gerufen. Ziel ist es, in den einzelnen Gesundheitsregionen eine bedarfsdeckende und möglichst wohnortnahe Gesundheitsversorgung der Bürgerinnen und Bürger zu ermöglichen. Daten über die Gesundheit eines Menschen gehören zu den sensibelsten und schutzbedürftigsten. Daher lag es nahe, die Datenverarbeitung im Rahmen der Gesundheitsregionen in Niedersachsen zu prüfen.

Ziel meiner Prüfung war es, zu erfahren welche Projekte in den einzelnen Regionen durchgeführt werden und ob im Rahmen dieser Projekte auch personenbezogene Daten der Bürgerinnen und Bürger verarbeitet werden. Hierzu habe ich allen 35 anerkannten Gesundheitsregionen einen entsprechenden Fragebogen zukommen lassen. Zum Ende des Berichtszeitraums lagen mir noch nicht von allen Gesundheitsregionen Rückmeldungen vor, sodass eine abschließende Auswertung noch nicht vorgenommen werden konnte. Aus den bisher vorliegenden Antworten konnte ich entnehmen, dass die Projekte im Rahmen der Gesundheitsregionen in Niedersachsen von Informationsveranstaltungen zur landärztlichen Versorgungssituation bis hin zur Entwicklung von Gesundheits-Apps reichen. Sofern die Erhebung und Verarbeitung der personenbezogenen Daten Bestandteil eines Projektes sind, werde ich das weitere Vorgehen hinterfragen, die jeweilige Region detaillierter prüfen und bei Bedarf datenschutzrechtlich beraten.

Quelle: www.niedersachsen.de

Aufbauend auf den Auswertungsergebnissen werde ich im nächsten Berichtszeitraum auch Prüfungen vor Ort durchführen. Es ist mir wichtig, durch gezielte Informationen und Beratung einen datenschutzgerechten Umgang mit personenbezogenen Daten zu erreichen und das Bewusstsein aller Beteiligten für datenschutzrechtliche Belange zu stärken.

4.3 „Datenübermittlung zwischen Ärztinnen und Ärzten, Krankenkasse und dem Medizinischen Dienst der Krankenversicherung

Meine Behörde erreichte im Berichtszeitraum viele Anfragen zu dem sogenannten Umschlagverfahren. Bei dem Datenaustausch zwischen Leistungserbringern wie Ärztinnen und Ärzten, den gesetzlichen Krankenkassen und dem Medizinischen Dienst der Krankenversicherung (MDK) gab es im Jahr 2016 vermehrt Unsicherheiten auf Seiten der Leistungserbringer, wie diese sich datenschutzgerecht verhalten können.

Im Bereich des Sozialversicherungsrechts gelten besondere datenschutzrechtliche Regelungen. Die gesetzlichen Krankenkassen dürfen nur einen eng definierten Datenkatalog erheben. Arztberichte oder Krankenhausberichte, welche detaillierte Angaben zu einer Erkrankung der Versicherten enthalten, darf die Krankenkasse grundsätzlich nicht einsehen. Stellt die Krankenkasse bspw. eine Krankenhausrechnung in Frage oder sind Leistungsanträge der Versicherten genauer zu prüfen, ist es in vielen Fällen erforderlich, auch medizinische Berichte heranzuziehen. Aus diesem Grund hat der Gesetzgeber die gesetzlichen Krankenkassen verpflichtet, bestimmte Prüfungen vom MDK vornehmen zu lassen, welcher gesetzlich befugt ist, diese sensiblen Patientendaten sowohl zu erheben als auch zu verarbeiten.

Beim bisherigen Umschlagverfahren haben Leistungserbringer, insbesondere Ärztinnen und Ärzte, auf Anforderung der Krankenkasse medizinische Unterlagen und Befunde in einem verschlossenen Briefumschlag mit dem Hinweis „Nur vom MDK zu öffnen“ an die Krankenkasse übermittelt. Diese hat die ungeöffneten Umschläge zusammen mit einem Prüfauftrag an den MDK weitergeleitet. Erst die Gutachter beim MDK durften Einsicht in die medizinischen Unterlagen nehmen.

Eine großflächig angelegte Prüfung verschiedener gesetzlicher Krankenkassen durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führte zu dem Ergebnis, dass in der täglichen Praxis viele Umschläge nicht korrekt verschlossen bzw. sogar geöffnet in den Akten der Krankenkassen vorhanden waren. Die Krankenkassen konnten somit unzulässiger Weise hochsensible Gesundheitsdaten ihrer Versicherten einsehen.

Umschlagverfahren nach Hinweisen der Datenschutzbehörde abgeschafft

Zu Beginn des Jahres 2016 hat der Gesetzgeber auf entsprechende Hinweise der Aufsichtsbehörde reagiert und die Datenübermittlung im Rahmen des Um-

schlagverfahrens durch eine Gesetzesänderung abgeschafft. Seitdem müssen die Leistungserbringer die medizinischen Daten direkt an den MDK übersenden. Damit der MDK die Eingänge der verschiedenen Leistungserbringer einem konkreten Fall zuordnen kann, bedurfte es der Einführung eines neuen Verfahrens. Hierzu hat der MDK Bundesverband zugesagt, bis zum 31.12.2016 ein entsprechend datenschutzrechtlich sicheres elektronisches Verfahren zu entwickeln.

Da eine Entwicklung dieser Technik nicht innerhalb weniger Wochen möglich ist, haben sich die Datenschutzaufsichtsbehörden des Bundes und der Länder darauf verständigt, bis zur Umsetzung eines elektronischen Verfahrens durch den MDK das bisherige Verfahren bis Ende 2016 zu tolerieren und keine Beanstandung auszusprechen, sofern das Verfahren ordnungsgemäß mit verschlossenen Umschlägen durchgeführt wird. In Niedersachsen gab es in diesem Bereich keine Beanstandungen.

Diese neue Art der direkten Übermittlung der Daten ohne den Umweg über die Krankenkasse begrüße ich sehr. Das Risiko einer ungewollten Datenübermittlung, durch einen aus Versehen geöffneten Umschlag, entfällt zukünftig. Jede Minimierung von Risiken bei der Datenübermittlung ist ein Gewinn für das informationelle Selbstbestimmungsrecht der Betroffenen. Dies gilt selbstverständlich auch für die technische Umsetzung dieses neuen Verfahrens.

Neben dem Vorteil der Risikominimierung gehe ich davon aus, dass die künftige elektronische Übermittlung für alle Beteiligten einen deutlichen Zeitgewinn und eine Arbeitserleichterung mit sich bringen wird.

Zum Ende des Berichtszeitraums wurde in Niedersachsen bereits begonnen, die Einführung des elektronischen Verfahrens umzusetzen. Die Ablösung des Umschlagsverfahrens ist größtenteils zum Jahreswechsel erfolgt. Wie sich das neue Verfahren in der Praxis bewährt, werde ich in den nächsten Jahren aufmerksam verfolgen.

4.4 „Mitteilungspflichten des MDK“

Übermittlung von Gutachten an die Krankenkasse

Immer wieder stellt sich den Beschäftigten bei der Krankenkasse und dem Medizinische Dienst der Krankenversicherung in Niedersachsen (MDK) die Frage, in welchem Umfang der MDK sozialmedizinische Gutachten an die jeweiligen Krankenkassen und Leistungserbringer wie Ärztinnen und Ärzte weiterleiten darf.

§ 277 SGB V regelt die Mitteilungspflichten des MDK gegenüber den Krankenkassen und Leistungserbringern. Damit hat der Gesetzgeber eine Grundlage für die Übermittlungspflichten und die Übermittlungsbefugnisse des MDK geschaffen und den Zugang der Krankenkassen zu medizinischen Detailinformationen sehr eingeschränkt erlaubt.

Auszug - § 277 Abs. 1 Sätze 1 bis 3 SGB V

Der Medizinische Dienst hat dem an der vertragsärztlichen Versorgung teilnehmenden Arzt, sonstigen Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, und der Krankenkasse das Ergebnis der Begutachtung und der Krankenkasse die erforderlichen Angaben über den Befund mitzuteilen. Er ist befugt, den an der vertragsärztlichen Versorgung teilnehmenden Ärzten und den sonstigen Leistungserbringern, über deren Leistungen er eine gutachtliche Stellungnahme abgegeben hat, die erforderlichen Angaben über den Befund mitzuteilen. Der Versicherte kann der Mitteilung über den Befund an die Leistungserbringer widersprechen. […]

Der Umfang und der Inhalt des MDK-Gutachtens ist immer abhängig von der beantragten Leistung der Versicherten und der diesbezüglichen Fragestellung der Krankenkasse.

Bereits bei der Erstellung haben die Gutachter auf die erforderlichen Angaben abzustellen und das Sozialgeheimnis zu beachten. Die Übersendung des gesamten Gutachtens an die Krankenkasse ist ungeachtet dessen datenschutzrechtlich unzulässig.

Der MDK hat lediglich das abschließende Ergebnis und die erforderlichen Angaben über den Befund gegenüber der Auftrag gebenden Krankenkasse mitzuteilen. Hinzu kommt eine sozialmedizinische Empfehlung und sofern erforderlich, eine sozialmedizinische Beurteilung.

Der Umfang der Befundmitteilung für die Krankenkasse hat sich daran zu orientieren, dass die Krankenkasse im Rahmen einer Leistungsablehnung an den Versicherten in die Lage versetzt wird, einen Verwaltungsakt rechtlich hinreichend bestimmt zu begründen.

Gegenüber den Leistungserbringern ist der MDK datenschutzrechtlich befugt, aber nicht verpflichtet, Angaben zum Befund mitzuteilen. Die Entscheidung, ob eine Unterrichtung an die Leistungserbringer erfolgt, obliegt dem MDK. Der Mitteilung über den Befund (nicht die Ergebnismitteilung) können die Versicherten jedoch widersprechen.

4.5 Projekt „Datenschutzrechtliche Prüfung von Wearables“

Im Rahmen der 91. Sitzung der DSK im März 2016 wurde das Projekt „Datenschutzrechtliche Prüfung von Wearables“ initiiert, da Wearables in weiten Kreisen der Bevölkerung immer stärker genutzt werden. Ziel des Projektes war es, ausgewählte Wearables (hier: Fitnessbänder und Smart Watches) unter Datenschutzaspekten technisch und juristisch zu prüfen. Dazu wurden für die jeweiligen Prüfungen eigene Kataloge erstellt.

An dem Projekt beteiligten sich die Landesdatenschutzbehörden von Bayern, Brandenburg, Hessen, Niedersachsen, NRW, Schleswig-Holstein und die BfDI. Im Rahmen der Prüfung wurden einerseits die technischen Prüfungen und Analysen durchgeführt, andererseits wurden die juristischen Fragestellungen aufbauend auf den Ergebnissen der technischen Prüfung erörtert und bewertet.

Technische Prüfung

Prüfobjekte

Von den für die Prüfung ausgewählten 16 Wearables wurden in Niedersachsen drei Geräte einer intensiven Prüfung unterzogen. Die Geräte wurden bei einer Sporthandelskette, in einem Elektronikfachhandel und über das Internet zu einem Preis zwischen 65 und 115 Euro erworben. Damit wurde sichergestellt, dass die Hersteller nicht die Möglichkeit hatten, die Geräte speziell für die Prüfung vorzubereiten.

Bei den Geräten handelte es sich um Fitnessarmbänder, die sowohl tagsüber im Alltag und beim Sport, oder nachts im Schlaf am Arm wie eine Uhr getragen werden. Durch verschiedene eingebaute Sensoren waren die Geräte in der Lage sowohl Bewegungen zu ermitteln als auch Körperdaten (z.B. Puls) zu erfassen.
Die Nutzer können diese von den Wearables aufgezeichneten Daten auswerten, indem sie die von den Herstellern bereitgestellten Apps auf ihr Smartphone laden und dort installieren. Dann muss das Wearable mittels einer Funkverbindung (Bluetooth) mit dem Smartphone verbunden (gekoppelt) werden. Zusätzlich ist meistens die Anmeldung bzw. Registrierung innerhalb der App oder auf der Website des Herstellers notwendig.

Prüfungsaufbau

Die Prüfung wurde in dem im Jahr 2016 eingerichteten IT-Labor der LfD durchgeführt.
Neben den drei Prüfgeräten wurde ein Android-Smartphone (Huawei Nexus 6P, Android-Version 6.0.1), ein W-LAN Accesspoint und ein Analyserechner in geeigneter Weise untereinander und anschließend mit dem hauseigenen Internetanschluss verbunden.
Das Smartphone wurde zu Beginn der Prüfung „gerootet“, so dass der Zugriff auf den internen Speicher möglich wurde und anschließend mittels Bluetooth mit dem zu prüfenden Wearable gekoppelt. Der W-LAN-Accesspoint wurde so konfiguriert und in das Labornetz eingebunden, dass er die übertragenen Daten zwischen dem Smartphone und der Website des Herstellers über den Analyserechner leitete.

Auf dem Analyserechner, der unter dem Kali-Linux Betriebssystem betrieben wurde, wurden die Software Burp-Suite von Portswigger, der Datenbankbrowser SQLite sowie einige Tools zur Überprüfung der von der jeweiligen Website des Herstellers verwendeten Verschlüsselung für die Prüfung eingesetzt.

Prüfungsablauf

Die Prüfgeräte wurden sequentiell nacheinander geprüft.
Entsprechend der herstellerspezifischen Bedienungsanleitung wurden dazu die Wearables und die korrespondierende App vorbereitet.
Bei dieser Inbetriebnahme wurde überprüft, welche Datenschutzbestimmungen zu welcher Zeit dem Nutzer zur Kenntnis oder zur Genehmigung präsentiert wurden, welche Daten der Nutzer im Rahmen der Registrierung angeben musste und in welcher Art und Weise die App mit dem Server des Herstellers kommuniziert. Hierbei wurde besonders darauf geachtet, ob sensible Daten (Passwörter) übertragen wurden und welche Verschlüsselung genutzt wurde.
Nach Inbetriebnahme der Geräte erfolgte die bestimmungsgemäße Nutzung gemäß Herstellervorgaben über einen bestimmten Zeitraum hinweg. Anschließend wurde analysiert, welche Daten vom Wearable auf das Smartphone übertragen worden sind, welche Daten sich im (normalerweise nicht zugänglichen) internen Speicher des Smartphones befanden und welche Daten über das Internet an Dritte versendet wurden.

Abschließend wurde sowohl die App auf dem Smartphone gelöscht, als auch (soweit möglich), das Wearable zurückgesetzt.

Prüfergebnisse

Im Rahmen der technischen Prüfung der Wearables wurde festgestellt, dass durch die Wearables und die zugehörige App eine Vielzahl von personenbezogenen, aber auch geräteabhängigen (eindeutigen) Daten verarbeitet worden ist. Der sparsame Umgang mit (personenbezogenen) Daten konnte nicht festgestellt werden.

Da der Nutzer allerdings im Rahmen der Installation und Nutzung der App eine sehr weitreichende Einwilligung zur Erfassung und Verarbeitung der Daten erteilt hat, erfolgte die Verarbeitung innerhalb dieses sehr großzügigen Rahmens.

Es ist zu bemängeln, dass die vorhandenen Datenschutzbestimmungen auf der Website des Herstellers, im App-Store und innerhalb der App zum Teil unterschiedlich waren (unterschiedliche Sprachen, unterschiedliche Versionsstände).

Die Übertragung der Daten von der App an die Website der Hersteller erfolgte verschlüsselt. Allerdings wurden die Passwörter nur mittels Transportverschlüsselung (https) gesichert, nicht aber durch eine Verschlüsselung innerhalb der App und anschließende Übertragung der verschlüsselten Passwörter, so dass die Passwörter durch eine „Man in the Middle"-Konstellation im Klartext ausgelesen werden konnten.

Die Übertragung der erhobenen Daten ist zudem in den meisten Fällen gar nicht notwendig, da die Smartphones mittlerweile so leistungsfähig sind, dass die Daten auf dem Smartphone selbst verarbeitet werden können.

Rechtliche Prüfung

Fragestellungen

Das Hauptaugenmerk bei der juristischen Prüfung lag auf der Analyse der Nutzungs- und Datenschutzbedingungen. Angesichts der ausnahmslos ausländischen Hersteller/Anbieter der durch Niedersachsen getesteten Geräte stellten sich zunächst durchweg die Fragen der Anwendbarkeit deutschen Rechts und der aufsichtsrechtlichen Zuständigkeit der Landesdatenschutzbeauftragten – oder überhaupt einer deutschen Aufsichtsbehörde. Diese vorausgesetzt, war auch zu bewerten, ob die durch Wearables (und Apps) erhobenen und weiterverarbeiteten Daten der Kategorie der besonderen Arten personenbezogener Daten gem. § 3 Abs. 9 BDSG angehören; es könnte sich durchweg um „Angaben über die Gesundheit" im Sinne der Norm handeln. Die Konsequenz wäre, dass in jedem Falle eine wirksame datenschutzrechtliche Einwilligung explizit bezogen auf diese Daten einzuholen wäre – die Verarbeitung allein auf Grundlage des § 28 Abs. 1 Nr. 1 BDSG, mit einer Regelung der Nutzungsbedingungen in Form von allgemeinen Geschäftsbedingungen (AGB), wäre ausgeschlossen. Neben dem Abgleich der Angaben zur für die Nutzung der Wearables übermittelten Daten mit den (tatsächlichen) Ergebnissen der technischen Prüfung, war also zu bewerten, inwiefern die Bestimmungen eine ausreichende Rechtsgrundlage für die Datenverarbeitung darstellen und ob die europäischen Nutzern bekannten „klassischen" Betroffenenrechte, etwa auf Auskunft über die zur eigenen Person gespeicherten Daten und gegebenenfalls Löschung dieser, gewährleistet werden.

Datensparsamkeit war gestern

Positiv ist zunächst zu bemerken, dass keine Datenerhebungen und –übermittlungen durch die getesteten Wearables und die dazugehörigen Smartphone-Apps technisch festgestellt wurden, die nicht auch in den Datenschutzbestimmungen oder wenigstens in den Übersichten zu den erforderlichen Berechtigungen aufgeführt waren. Datenschutzrechtlich bestand deswegen dennoch kein Grund zur Freude, da die einzuräumenden Berechtigungen schlicht sehr umfassend und die Datenschutzbestimmungen weit und größtenteils auch schwammig formuliert waren. Ein Grundprinzip des Datenschutzes – die Datensparsamkeit – war bei keinem getesteten Gerät Leitprinzip der Entwicklung; soviel ist festzuhalten.
Nun ist grundsätzlich anzuerkennen, dass Menschen ein Wearable (gerade) deshalb nutzen, weil sie sich selbst vermessen und – möglicherweise – die Ergebnisse auswerten lassen und mit anderen vergleichen wollen. Datensparsamkeit ist aus dieser Perspektive heraus eher kontraproduktiv. Natürlich muss man dem Smartphone erlauben, den eingebauten GPS-Sender einzuschalten und die so gemessenen Standortdaten an den Server des Herstellers des Wearables zu übermitteln, wenn man live beim Joggen getrackt werden und dies z.B. mit Freunden in einem sozialen Netzwerk teilen möchte. Diese umfassende Datenverarbeitung ist in diesem Falle erforderlich. Anders geht es technisch nicht. Grundsätzlich wäre aber die lokale Verarbeitung der Standortdaten technisch möglich. Der Nutzer könnte dann in einem weiteren Schritt selbst entscheiden, ob er

Messdaten an den Hersteller übermitteln möchte. In jedem Fall gebietet es das Grundrecht auf informationelle Selbstbestimmung, zu gewährleisten, dass Nutzende bei ihrer selbstgewählten Selbstvermessung über Art, Umfang und Zwecke der hierzu und hierbei erfolgenden Datenerhebung informiert sind. Entscheidend war aus rechtlicher Sicht daher, ob die Datenschutz- und Nutzungsbestimmungen die an Klarheit und Vollständigkeit zu stellenden Anforderungen erfüllen; ob die Nutzenden auf ihrer Grundlage eine informierte und freiwillige Entscheidung über die vollständige durch die Anbieter vorgenommene Datenverarbeitung treffen können.

Gesundheitsdaten

Die getesteten Geräte und Apps werden herstellerseitig durchweg mit Bezeichnungen wie „Fitness-Tracker" oder „Schlaf-Tracker" beworben. Ihre Hauptfunktionen sind die Messung von „Körper- und Bewegungsdaten". Zunächst handelt es sich dabei um – isoliert betrachtet – Einzelinformationen wie zurückgelegte Schritte, Herzfrequenz und Schlafdauer. Über die Zeit und in Kombination mit den Daten, die die Nutzenden für brauchbare Ergebnisse regelmäßig zusätzlich eingeben sollen (Körpergewicht, Größe, Alter etc.) ermöglicht die Zusammenschau der Daten aber sehr individuelle Informationen über Gewohnheiten und auch physischen und psychischen Zustand der Nutzenden.

Aus rechtlicher Sicht war daher zu bewerten, ob es sich um gesetzlich besonders geschützte „Gesundheitsdaten" handelt. „Gesundheitsdaten" sind im bisher geltenden deutschen Recht nicht legal definiert. Auf europäischer Ebene hat die Arbeitsgruppe der europäischen Datenschutzbeauftragten (Art. 29 Working Party) jedoch bereits 2015 in einer Stellungnahme eine sehr weite Definition vertreten. Hiernach sind jedenfalls medizinische Daten, die in einem professionellen medizinischen Kontext generiert werden, nur ein Teil der Gesundheitsdaten. Der datenschutzrechtliche Begriff der Gesundheitsdaten soll indes auch Daten über den physischen oder psychischen Zustand hinaus umfassen, selbst wenn sie nur bedingt im Zusammenhang mit einem medizinischen Kontext entstehen. Dazu zählen etwa Informationen über einen Beinbruch, das Tragen einer Brille oder Kontaktlinsen, über intellektuelle oder mentale Fähigkeiten, Trink- oder Rauchverhalten, Allergien oder Teilnahme an einer Selbsthilfegruppe. Diese Beispiele umfassen bereits nicht nur Vitaldaten, sondern auch Daten, die nur mittelbar – insbesondere aufgrund eines bestimmten Zusatzwissens und durch ihre gezielte Auswertung – einen Rückschluss auf den Gesundheitszustand der Person zulassen. So lässt sich z. B. selbst aus einer verhältnismäßig hohen Gewichtsangabe nur ein Rückschluss auf ein gesundheitsbeeinträchtigendes Übergewicht ziehen, wenn insbesondere Größe, Alter und Geschlecht der Person bekannt sind. Tägliche Schrittzahlen können durch Kombination mit weiteren Informationen der Person, wie der Pulsfrequenz, eine Aussage über den Gesundheitszustand des Herz-Kreislaufsystems treffen. Würde die Schrittzahl nicht mit anderen Daten des Nutzers kombiniert und die App nicht in einem speziellen medizinischen Kontext benutzt, wären die Daten (als bloße „well being data") keine Gesundheitsdaten. Dieser Ansatz, dass die Datenerhebung nicht (von Anfang an) in einem medizinischen Kontext stehen muss, wird jedenfalls durch die DS-GVO ab Mai 2018 geltendes Recht sein. Die DS-GVO definiert in Art. 4 Nr. 15 Gesundheitsdaten (erstmals) legal als „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen." In Erwägungsgrund 35 der DS-GVO wird erläutert: „Zu den personenbezogenen Gesundheitsdaten sollten alle Daten zählen, die sich auf den Gesundheits-

zustand einer betroffenen Person beziehen und aus denen Informationen über den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen." Und sodann: „Dazu gehören auch Informationen über die natürliche Person, die im Zuge der Anmeldung für sowie der Erbringung von Gesundheitsdienstleistungen (…) für die natürliche Person erhoben werden (…)".Wegen dieser Einordnungsprobleme ist unter Berücksichtigung des datenschutzrechtlichen Vorsorgegedankens anzunehmen, dass bereits bei der hypothetischen Möglichkeit einer Kombination und Auswertung von Gesundheitsdaten auszugehen ist. Aufgrund der immer weitergehenden technischen Entwicklungen wird es zunehmend möglich sein, aus fast jedem Datum Rückschlüsse auf die Gesundheit einer Person zu ziehen.
Rechtsgrundlagen

Nationales Recht

Die getesteten Wearables waren allesamt Produkte nordamerikanischer Hersteller; die dazugehörigen Apps wurden ebenso von den jeweiligen Herstellern angeboten. Es stellte sich mithin auch die Frage, ob überhaupt deutsches Recht anwendbar ist. Unter Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs in den letzten Jahren war diese Frage durchweg mit „nein" zu beantworten. Alle Anbieter im Test hatten Hauptniederlassungen in anderen europäischen Mitgliedstaaten – namentlich Großbritannien und Irland – was zu einer Anwendbarkeit britischen bzw. irischen Datenschutzrechts führt. Bei einer Beschwerde eines niedersächsischen Bürgers wäre die Landesdatenschutzbeauftragte zwar berechtigt, die Beschwerde anhand des anwendbaren Rechts (britisch oder irisch) zu prüfen; für jegliches hoheitliches Handeln – sei es auch nur das Verlangen nach Auskunft gegenüber den jeweiligen Unternehmen – müsste sie jedoch die Datenschutzbeauftragten in Großbritannien bzw. Irland um Amtshilfe ersuchen oder den Fall an diese abgeben.
Anders wäre der Sachverhalt jedoch zu beurteilen, wenn beispielsweise eine in Niedersachsen ansässige Krankenkasse ihren Versicherten ein Wearable zur Verfügung stellt bzw. Vergünstigungen bei Übermittlung der hiermit gemessenen Werte offeriert. Da erste Versicherer solche Programme testen, erschien die Beschäftigung mit der zugrundeliegenden Technik und der Thematik für die Landesdatenschutzbeauftragte auch so mehr als geboten.

Einwilligung

Wenn Gesundheitsdaten verarbeitet werden sollen, ist hierzu nach deutschem Recht immer die ausdrückliche Einwilligung der Betroffenen erforderlich (§ 4a Abs. 3 BDSG). Dies entspricht der Vorgabe der europäischen „Datenschutzrichtlinie" (Art. 8 Abs. 2 95/46/EG).

Bei keinem der getesteten Produkte wurde bei Installation der für den Gebrauch notwendigen App auf dem Smartphone oder vor Inbetriebnahme eine gültige Einwilligung der Nutzenden eingeholt. Für eine – bei der Verarbeitung von Gesundheitsdaten notwendige – explizit auf die Verarbeitung dieser Daten bezogene Einwilligung genügt das pauschale „Abhaken" der Datenschutzbestimmungen oder Nutzungsbedingungen nicht. Ein separater Passus zur Einwilligung in die Verarbeitung von Gesundheitsdaten wurde jedoch von keinem Anbieter vorgelegt.

Weiterhin muss eine Einwilligung „freiwillig und informiert" sein. Nutzende müssen über Art, Umfang und Zwecke der Datenverarbeitung informiert werden, bevor diese beginnt. Das heißt,

der Anbieter müsste umfassend und konkret informieren: Über alle Kategorien von Daten, die mit dem Wearable ermittelt und mittels der dazugehörigen App an ihn übertragen werden. Weiterhin müsste er darüber informieren, dass die durch das Wearable ermittelten Daten mit durch das Smartphone bzw. die App erhobenen Daten (z.B. Standortdaten, aber auch Gerätedaten und sonstige Verbindungs- und Nutzungsdaten) verknüpft werden, sofern dies erfolgt. Der Anbieter müsste erläutern, was genau er mit den übermittelten Daten macht – welche Auswertungen stattfinden, ob er diese selbst vornimmt oder hierzu einen Auftragsdatenverarbeiter einsetzt, ob er Daten an Dritte weitergibt (als Rohdaten oder als Profil; pseudonymisiert oder sogar mit Klarnamen?) und wenn, zu welchen Zwecken. Er müsste auch angeben, wie lange er die Daten als personenbeziehbare Daten speichert – und wo. Die Tatsache der Übermittlung ins Nicht-EU-Ausland sollte ebenso offenbart werden, wie das genaue Empfängerland.

Die Beispiele sind nicht abschließend. Keines der getesteten Geräte war mit Bestimmungen versehen, die die inhaltlichen gesetzlichen Anforderungen auch nur ansatzweise erfüllt hätten. Datenschutzerklärungen beschränkten sich – sofern überhaupt konkret auf das Wearable und die dazugehörige App bezogen – auf pauschale Hinweise, die es Nutzenden keinesfalls ermöglichen, einzuschätzen, wer in welchem Umfang Zugang zu ihren Daten erhält und zu welchen Zwecken sie verarbeitet werden. Die Weitergabe an (unbestimmte) Dritte wird ohne Widerspruchsmöglichkeit vorbehalten; ein weiterer Verstoß gegen europäisches Recht.

Auch formal entsprach keine der Datenschutzerklärungen den Anforderungen an die „allgemein verständliche Form“; sie waren ausgedruckt bis zu zehn DIN A 4-Seiten lang, teils nicht auf Deutsch verfügbar und enthielten größtenteils zahlreiche juristische Fachbegriffe.

Zusammenfassend

Aus Sicht des Datenschutzes entsprach kein Gerät den Anforderungen, die technisch-organisatorisch an es zu stellen sind. Zunächst ist es möglich eine nur lokale Verarbeitung der Daten auf dem Smartphone zu implementieren. Für die meisten Zwecke ist dies ausreichend, gibt dem Nutzenden die effektive Kontrolle über seine eigenen Daten und erfüllt den Grundsatz der Datensparsamkeit.

Da viele der durch die getesteten Geräte und die dazugehörigen Apps verarbeiteten Daten als Gesundheitsdaten einen hohen bis sehr hohen Schutzbedarf haben, wäre bei der festgestellten Implementierung die Verschlüsselung der Daten vor Übertragung erforderlich.

Aus rechtlicher Sicht ist insbesondere die mangelhafte Aufklärung der Nutzenden in den Datenschutzerklärungen zu beanstanden. Nutzende müssen wissen, welche ihrer personenbezogenen Daten durch wen und wozu verarbeitet werden. Wenn dies nicht erfolgt, ist eine Einwilligung als Rechtsgrund für die Verarbeitung unwirksam. Im Ergebnis konnte daher auch bei keinem der getesteten Geräte zum Kauf geraten werden.

4.6 Jobcenter und Sozialämter verlangen Vermieterbescheinigungen

Seit einigen Jahren erhalte ich regelmäßig Eingaben, in denen sich Antragstellerinnen und Antragsteller von Sozialleistungen beschweren, dass die Jobcenter und Sozialämter im Rahmen der Antragstellung eine Bescheinigung der Vermieterin oder des Vermieters einer Wohnung verlangen und die Beibringung dieser Bescheinigung zu den sanktionsbewehrten Mitwirkungspflichten zählen.
Die hierzu überreichten Vordrucke offenbaren teilweise schon vom Layout den Sozialleistungsbezug.

Das Sozialamt ist nach § 67a Absatz 1 Satz 1 SGB X berechtigt, Sozialdaten zu erheben, soweit dies für die Erfüllung seiner Aufgaben nach dem Sozialgesetzbuch erforderlich ist.

Nach § 67a Absatz 2 Satz 1 SGB X sind Sozialdaten vorrangig bei den Betroffenen zu erheben. Den Antragstellenden ist somit Gelegenheit zu geben, die erforderlichen Daten durch geeignete Nachweise selbst zu erbringen.

Mit dem Vordruck der Vermieterbescheinigungen beabsichtigt der Leistungsträger die für die Feststellung der Anspruchsvoraussetzungen nach dem SGB II oder SGB XII erforderlichen Daten zu erheben. Den Großteil der Daten können die Antragstellenden mit eigenen Unterlagen, wie beispielsweise dem Mietvertrag oder der Nebenkostenabrechnung, nachweisen.

Einige Daten werden die Antragstellenden jedoch nicht kennen und somit auch nicht nachweisen können. Bei diesen Daten handelt es sich zum Beispiel um Angaben, mit welchen die Heizkosten überprüft werden sollen. In einem ungedämmten Gebäude sind die Heizkosten deutlich höher, als in einem frisch sanierten Gebäude. Die fehlende Dämmung darf jedoch nicht als unwirtschaftliches Heizen und somit zu Lasten der Betroffenen ausgelegt werden. Zur Prüfung, ob die verursachten Heizkosten angemessen sind, gibt es jedoch in der Regel bereits statistische Durchschnittswerte, welche vorrangig heranzuziehen sind.

Zum einen ist die Heranziehung von Durchschnittswerten immer ein wesentlich milderes Mittel als die Offenbarung des Sozialleistungsbezuges der Betroffenen gegenüber den Vermietern, zum anderen wäre eine Forderung der von den Vermietern ausgefüllten Vermieterbescheinigung im Rahmen der Mitwirkungspflichten nach § 60 ff. SGB I nur dann zulässig, wenn den Antragstellenden die Erfüllung der Vorlagepflicht objektiv möglich wäre.

Es besteht jedoch keine gesetzliche Verpflichtung für die Vermietenden, die Vermieterbescheinigung auszufüllen oder in irgendeiner Art und Weise an

dem Antragsverfahren der Betroffenen mitzuwirken. Damit ist die Erfüllbarkeit der Anforderung der Vermieterbescheinigung von der Kooperationsbereitschaft der Vermieter abhängig. Sollten die Vermietenden das Ausfüllen der Vermieterbescheinigung verweigern, wird den Antragstellenden die Vorlage beim Jobcenter unmöglich.

Aus diesem Grund kann die Vorlage einer von den Vermietenden ausgefüllten Vermieterbescheinigung nicht zu den Mitwirkungspflichten gezählt werden. Die Vermieterbescheinigung kann demnach lediglich ein zusätzliches, freiwilliges Angebot zum Nachweis ergänzender Informationen darstellen.

Des Weiteren wäre mit einer Verpflichtung zur Vorlage der Vermieterbescheinigung ebenfalls eine Verpflichtung zur Offenlegung des Sozialleistungsbezuges der Betroffenen gegenüber den Vermietenden verbunden. Wie bereits dargestellt, ist davon auszugehen, dass die mit einer Vermieterbescheinigung erhobenen Daten überwiegend auch auf andere Weise erhoben werden können. Die Preisgabe des Sozialleistungsbezuges ist daher nicht erforderlich und stellt eine Überschreitung der Grenzen der Mitwirkungspflichten nach § 65 Absatz 1 Nr. 1 SGB I dar. Eine Androhung von Sanktionen gegenüber den Antragstellenden ist somit nicht zulässig.

Leittext des Urteils des Bundessozialgerichts vom 25.01.2012
Der Bezug von Sozialhilfe oder Arbeitslosengeld II ist ein Sozialdatum, dessen Offenbarung durch das Jobcenter nur zulässig ist, wenn der Leistungsbezieher eingewilligt hat oder eine gesetzliche Offenbarungsbefugnis vorliegt
(BSG, 25.01.2012 - Az.: B 14 AS 65/11 R).

5. Datenschutzbeauftragte

5.1 Datenschutzbeauftragte in Schulen – immer noch eine Vielzahl weißer Flecken auf der Landkarte

An Schulen werden täglich eine Vielzahl sensibler personenbezogener Daten verarbeitet. Ich habe das Niedersächsische Kultusministerium (MK) bereits vor vielen Jahren darauf hingewiesen, dass die Schulen als verantwortliche Stellen nach § 8 a NDSG Datenschutzbeauftragte bestellen müssen. Diese haben primär die Aufgabe, die Schule bei der Sicherstellung des Datenschutzes zu unterstützen. Eine von mir bereits im Jahr 2014 begonnene stichprobenartige Überprüfung der niedersächsischen Schulen hat aber ergeben, dass fast die Hälfte aller überprüften Schulen immer noch keine Datenschutzbeauftragten hat.

Auch im Berichtszeitraum ist meine Behörde mehrmals an das MK herangetreten und hat um eine zeitnahe Umsetzung der gesetzlichen Vorgabe zur Bestellung von Datenschutzbeauftragten in den Schulen gebeten. Das MK hat mir daraufhin ein Konzept zur Stärkung des schulischen Datenschutzes vorgelegt. Nach diesem Konzept sollten zunächst in jeder der vier Regionalabteilungen der Niedersächsischen Landesschulbehörde zwei Dezernentinnen oder Dezernenten für Datenschutzangelegenheiten der Schulen eingestellt werden, die die Schulen in datenschutzrechtlichen Fragen beraten. In weiteren Schritten sollen die Schulen bei der Bestellung eigener Datenschutzbeauftragter unterstützt werden.

Im Jahr 2016 wurden zwei Dezernentenstellen in den Regionalabteilungen der Landesschulbehörde in Hannover und Osnabrück besetzt. Zwei weitere Planstellen sind für die Regionalabteilungen Braunschweig und Lüneburg im Haushalt 2017/2018 ausgewiesen. Ob das MK beabsichtigt, die übrigen vier Datenschutzstellen des Konzeptes zeitnah zu besetzen, ist unklar.

Die Besetzung der Dezernentenstellen für schulischen Datenschutz in der Landesschulbehörde begrüße ich sehr. Dies bedeutet eine wichtige Unterstützung der Schulen bei der Umsetzung der gesetzlichen Vorgaben. Zudem haben sich im Berichtszeitraum gute Ansätze eines kooperativen Zusammenwirkens mit meiner Behörde ergeben. Gleichwohl führt dies nicht zu einer Befreiung

der Schulen von der gesetzlichen Verpflichtung zur Bestellung eigener Datenschutzbeauftragter. Ich habe dem MK mehrfach mitgeteilt, dass das vorgelegte Konzept nur eine zögerliche und inhaltlich unkonkrete Umsetzung der gesetzlichen Vorgabe bedeutet. Ein Hinausschieben der Bestellung von Datenschutzbeauftragten an den Schulen um weitere Jahre ist aus datenschutzrechtlicher Sicht – insbesondere vor dem Hintergrund des verstärkten Einsatzes neuer Medien im Schulalltag und der daraus resultierenden Risiken für die Grundrechte der Schülerinnen und Schüler – keinesfalls hinnehmbar.
Ich erwarte, dass das MK im Rahmen der ihm übertragenen Rechtsaufsicht über die Schulen auf eine zeitnahe Umsetzung der gesetzlichen Vorgabe zur Bestellung schulischer Datenschutzbeauftragter hinwirkt.

5.2 Ist die Bestellung einer juristischen Person (Rechtsanwalts-Partnerschaft) zum Datenschutzbeauftragten möglich?

In der datenschutzrechtlichen Kommentarliteratur wird verschiedentlich die Ansicht geäußert, dass eine Rechtsanwalts-Partnerschaftsgesellschaft im Sinne des Partnerschaftsgesellschaftsgesetzes (PartGG) als externer betrieblicher Datenschutzbeauftragter (bDSB) bestellt werden kann. So erreichte mich im Berichtszeitraum die Anfrage einer Rechtsanwaltskanzlei zur Zulässigkeit einer solchen Bestellung.

Da mehrere Datenschutzaufsichtsbehörden diese Anfrage erreicht hat, haben diese die aufgeworfene Rechtsfrage in einer Sitzung im Juni 2016 ausführlich erörtert, allerdings ohne Verständigung auf eine einheitliche Position. Daher möchte ich an dieser Stelle meine eigene Auffassung zu dieser Frage erläutern.

Die Auffassung der LfD Niedersachsen

Die von mir zu dieser Rechtsfrage vertretene Auffassung orientiert sich am Wortlaut der einschlägigen Normen des BDSG.
Nach § 4f Abs. 1 S.1 BDSG hat die verantwortliche Stelle einen Beauftragten für den Datenschutz zu bestellen, der nach § 4f Abs. 2 S.1 BDSG die erforderliche Fachkunde und Zuverlässigkeit aufweisen muss. Er ist in der Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei (§ 4f Abs. 3 S.2 BDSG). Diese Regelungen beziehen sich unstreitig auf natürliche Personen und gelten daher auch für solche Personen, die als bDSB nicht zugleich Mitarbeiter der verantwortlichen Stelle sind (sog. externe bDSB,
§ 4f Abs. 2 S.3 BDSG).

§§ 4f und 4g BDSG sind zudem jeweils auf eine einzelne natürliche Person hin formuliert. Eine verantwortliche Stelle, die einen bDSB zu bestellen hat, kann weder in- noch extern mehrere Personen zum bDSB bestellen, selbst wenn ihnen jeweils ein abgegrenzter eigener Zuständigkeitsbereich zugewiesen würde. Dies folgt nicht zuletzt aus § 4f Abs. 5 S.1 BDSG, wonach dem bDSB Hilfspersonal zur Verfügung zu stellen ist, sofern dies zur Erfüllung seiner Aufgaben erforderlich ist.

Insbesondere aus den Anforderungen im § 4f Abs. 2 S.1 BDSG an die Zuverlässigkeit und Fachkunde folgt, dass es sich dabei um persönliche Eigenschaften[1] handelt, die nur von natürlichen Personen erfüllt werden können. Bereits dieser Umstand schließt somit die Bestellung einer juristischen Person auch in der

1 So auch: Gola/Schomerus, Kommentar zum BDSG, 11. Aufl., §4f Rdnr. 19 m.w.N.

Form einer Partnerschaftsgesellschaft aus. Diese rechtliche Beurteilung findet ihre Bestätigung in einem Urteil des Landgerichts Ulm vom 30.10.1990 zur Fachkunde (Az.: 5T 153/90-01). Darin wird ausdrücklich die von mir vertretene Auffassung bestätigt, dass nur eine natürliche Person in der Lage ist, den „Beruf des Datenschutzbeauftragten" auszuüben. Nur diese kann die nötigen persönlichen Merkmale der Fachkunde und Zuverlässigkeit aufweisen und damit eine vertrauensvolle Zusammenarbeit der Beteiligten gewährleisten.
Das gefundene Ergebnis folgt im Übrigen auch aus § 4f Abs. 3 S1 BDSG, der eine unmittelbare Verantwortlichkeit des bDSB gegenüber der verantwortlichen Stelle vorsieht. Diese kann nur von einer natürlichen Person verwirklicht werden.

Partnerschaftsgesellschaftsgesetz führt zu keiner anderen Beurteilung

Eine andere Beurteilung der Rechtslage ist auch nicht unter Berücksichtigung des PartGG gerechtfertigt.
Eine Partnerschaft ist eine Gesellschaft, in der sich Angehörige freier Berufe zur Ausübung ihrer Berufe zusammenschließen (§ 1 Abs. 1 S.1 PartGG).Dabei ist die Ausübung eines freien Berufes i.S.d. PartGG die selbstständige Berufstätigkeit der dort genannten 24 freien Berufe einschließlich der Mitglieder der Rechtsanwaltskammern […] und „ähnlicher" Berufe sowie Wissenschaftler etc. (§ 1 Abs. 1 S.2 PartGG). Freie Berufe mit einem Bezug zum Datenschutz sind allerdings nicht genannt.

Damit erlangt die Frage, ob wegen der Regelungen im PartGG eine Bestellung der juristischen Person „Partnerschaft" zum bDSB möglich ist, nur dann Bedeutung, wenn der externe bDSB ein „ähnlicher" Beruf i.S.d. PartGG ist. Eine solche Ansicht wird in der Fachliteratur nicht vertreten. Vielmehr hat der BFH mit Urteil vom 05.06.2003 (Az. IV R 34/01) für eine vergleichbare Regelung in § 18 Abs. 1 Nr.1 S.2 EStG entschieden, dass ein externer bDSB kein Beruf ist, der dem des Freiberuflers „ähnlich" ist.
Ausnahmefälle sind nach einer Einzelfallprüfung nur dann vorstellbar, wenn ein namentlich bestimmter Mitarbeiter der Partnerschaft zum bDSB bestellt wird.

Keine abweichende Rechtsprechung nach Inkrafttreten der EU-DS-GVO

Die ab dem 25.05.2018 anwendbare EU-DS-GVO wird voraussichtlich zu keinem anderen Ergebnis führen. Die Vorschriften zum bDSB im 4. Abschnitt der DS-GVO enthalten jedenfalls im Hinblick auf die zur Diskussion gestellte Fragestellung keine Regelungen, die von denen im BDSG im Kern abweichen.

In meiner aufsichtsbehördlichen Praxis werde ich daher auch künftig nur die Bestellung von natürlichen Personen zum bDSB akzeptieren, die zudem die erforderliche Fachkunde und Zuverlässigkeit aufweisen müssen.

6. Datenschutz in der Wirtschaft

6.1 Anlassfreie Prüfungen bei Freizeit- und Indoorspielparks

Anlassfreie Prüfungen sind dadurch gekennzeichnet, dass im Rahmen von Stichprobenkontrollen mehrere Unternehmen einer Branche bzw. mit einem spezifischen Geschäftsmodell geprüft werden, ohne dass bereits im Vorfeld konkrete Anhaltspunkte für Datenschutzverstöße gegeben sind. Dabei können einzelne Aspekte eines komplexen Datenverarbeitungsprozesses, aber auch das gesamte Datenverarbeitungsmanagement Prüfungsgegenstand sein.
Im Berichtszeitraum habe ich mich auch der Freizeit- und Indoorspielparks in Niedersachsen gewidmet und den Stand der Umsetzung datenschutzrechtlicher Vorschriften abgefragt. Hierzu habe ich in zwei Schritten schriftliche Prüfungsaktionen bei 35 Freizeit- und Tierparks sowie bei 24 Indoorspielparks durchgeführt.

Bei anlassfreien Prüfungen erhalten die kontrollierten Unternehmen ein Schreiben und einen Fragenkatalog, den sie üblicherweise innerhalb von einem Monat – teilweise mit Vorlage relevanter Dokumente – beantworten und an mich zurücksenden müssen. Darüber hinaus verweise ich in meinen Schreiben auf umfangreiche Informationen, die von meinem Internetauftritt abgerufen werden können und in denen die abgefragten Sachverhalte detailliert erläutert werden.

Die Prüfung hat – wie häufig bei anlasslosen Prüfungen – zunächst ergeben, dass auch bei den Freizeit- und Indoorparks deutlicher Verbesserungsbedarf im Umgang mit personenbezogenen Daten bestand und die Kontrollen bei diesen häufig inhabergeführten und zum Teil sehr kleinen Unternehmen viel Grundberatung erforderten, um die Unternehmen datenschutzrechtlich auf den aktuellen Stand zu bringen.

Schwerpunkte der Prüfungen waren:

- die Ermittlung der datenschutzrechtlichen Rechtsgrundlagen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, auf die sich die Unternehmen insbesondere beim Umgang mit Kundendaten stützen
- die zu führenden Verfahrensverzeichnisse
- Datenverarbeitung durch externe Stellen und damit verbunden die Verträge über Auftragsdatenverarbeitung
- die Videoüberwachung einschließlich der konkret festgelegten Zwecke im Sinne von § 6b Abs. 1 Nr. 3 BDSG.

Konkret haben die schriftlichen Prüfungen ergeben, dass mehr als zwei Drittel der geprüften Unternehmen erst aufgrund meines Prüfungsanschreibens mit der Umsetzung der gesetzlichen Datenschutzanforderungen begonnen haben.
Allerdings hatten auch einige Unternehmen bereits grundlegende Vorgaben aus dem BDSG erfüllt, wie z. B. die Bestellung eines Datenschutzbeauftragten oder die Führung der entsprechenden Verfahrensverzeichnisse.
Leider überwogen aber die Lücken bei der Umsetzung des BDSG, die im Rahmen der Prüfung aufgearbeitet wurden. Nur bei sehr wenigen Unternehmen konnte die Prüfung ohne jede Beanstandung oder Hilfestellung meinerseits abgeschlossen werden.

Typische Mängel waren:

- Unzureichende oder überhaupt nicht vorhandene Verfahrensverzeichnisse sowie
- Nicht vorhandene Verträge zu Auftragsdatenverarbeitung.

Prüfungsgegenstand war in allen Fällen auch, ob eine Videoüberwachung von öffentlich zugänglichen Räumen i.S.d. § 6b BDSG erfolgt. Nach dieser Bestimmung ist die Beobachtung öffentlich zugänglicher Räume (z. B. Frei-

zeitflächen und Verkaufsräume) mit optisch-elektronischen Einrichtungen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Insgesamt haben 28 der 59 geprüften Unternehmen eine Videoüberwachung angegeben. Festgestellt habe ich, dass es einige Unzulänglichkeiten bei der Videoüberwachung gegeben hat. So fehlte häufig die nach § 6b Abs. 2 BDSG vorgeschriebene Hinweisbeschilderung. Der Erfassungsbereich einiger Kameras, die zum Teil auch Gastronomiebereiche erfassten, musste eingeschränkt werden. Auch die Löschfristen der überwiegend gespeicherten Videodaten bedurften in einigen Fällen der Reduzierung auf einen datenschutzgerechten Umfang, der in der Regel 48 Stunden nicht überschreiten darf.
Gravierende Verstöße oder nachhaltiges Verweigern, den Anforderungen der Datenschutzaufsicht Rechnung zu tragen, habe ich jedoch nur in zwei Fällen festgestellt, die mich zu datenschutzaufsichtlichen Folgemaßnahmen veranlassten.
Alle anderen Fälle hatten weder den Erlass von förmlichen Anordnungen mit dem Ziel einer datenschutzkonformen Nutzung von Videoüberwachungsanlagen noch den Erlass von Bußgeldbescheiden zur Folge.

Vereinzelte Prüfungen und Beratung vor Ort

In Einzelfällen wurden im Nachgang zu den schriftlichen Verfahren noch Vor-Ort-Prüfungen durchgeführt, um zu zeigen, dass Angaben auch im Praxisbetrieb überprüft werden. In einem Fall hat auf Bitten des Unternehmens auch eine umfassende zusätzliche Beratung vor Ort stattgefunden.
Insgesamt kann als positiv festgestellt werden, dass sich aufgrund meiner Prüfung sieben Unternehmen intensiv mit dem Thema Datenschutz auseinandergesetzt und in der Folge einen betrieblichen Datenschutzbeauftragten erstmals bestellt haben.

Das Ergebnis dieser aufsichtsbehördlichen Kontrolle hat gezeigt, dass solche Prüfungsaktionen eine geeignete Möglichkeit sind, um in einem überschaubaren Zeitraum einer größeren Zahl von Unternehmen das Thema Datenschutz näher zu bringen.
Mein Hauptziel ist es dabei stets, durch Information und Beratung einen gesetzeskonformen Umgang mit den persönlichen Daten insbesondere von Kunden und Mitarbeitern sowie eine angemessene Datenschutz- und Datensicherheitsorganisation zu erreichen und damit einen nachhaltigen Beitrag zur Verbesserung des Datenschutzniveaus in Unternehmen zu leisten.

6.2 Stichprobenverfahren: Vor-Ort-Prüfungen bei den Creditreformgesellschaften in Niedersachsen

Auch die niedersächsischen Creditreformgesellschaften (CRen) übermitteln ihren Geschäftspartnerinnen und -partnern (CR-Mitgliedern) gegen Entgelt u. a. Informationen über die Kreditwürdigkeit von Unternehmen oder Privatpersonen. Diese Weitergabe von personenbezogenen Daten erfolgt in automatisierten Verfahren und ist nur zulässig, wenn die Geschäftspartner ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt haben (§ 29 Abs. 2 Satz 1 Nr. 1 BDSG).
In diesem Zusammenhang haben sich die CRen stichprobenartig davon zu überzeugen, dass die Datenübermittlung ordnungsgemäß erfolgt ist (§ 29 Abs. 2 Satz 5 BDSG). Dazu ist in 2012 in Zusammenarbeit mit dem Verband der Vereine Creditreform (VVC) ein datenschutzkonformes Stichprobenkonzept erarbeitet worden. Im Berichtszeitraum hatten die niedersächsischen CRen Rechenschaft über ihre Handhabung dieses Stichprobenkonzeptes abzulegen.

Nach § 29 Abs. 2 Satz 1 Nr. 1 BDSG ist die Übermittlung personenbezogener Daten im Rahmen der Zwecke nach Absatz 1 (Tätigkeit von Auskunfteien) zulässig, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.
Diejenigen - also hier die CR-Mitglieder, die Daten von der Auskunftei erhalten, haben die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung aufzuzeichnen (§ 29 Abs. 2 Satz 3 und 4 BDSG).
Die übermittelnde Stelle - also hier z. B. eine CR - hat Stichprobenverfahren durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen (§ 29 Abs. 2 Satz 5 BDSG).

Datenschutzkonformes Stichprobenkonzept in 2012

Bereits in 2012 musste im Rahmen eines datenschutzrechtlichen Kontrollverfahrens bei einer der niedersächsischen CRen festgestellt werden, dass das dort bisher praktizierte Stichprobenkonzept nicht datenschutzkonform war. Daraufhin wurde in Kooperation mit dem VVC ein datenschutzkonformes Stichprobenkonzept erarbeitet. Auch für die weiteren niedersächsischen CRen wurde dieses neue Stichprobenkonzept für verbindlich erklärt.[1]

vgl. XXI Tätigkeitsbericht, S. 51 ff.

Eine spätere Überprüfung der jeweiligen Handhabung dieses neuen Stichprobenkonzepts durch die einzelnen CRen wurde angekündigt. Diese Überprüfung ist im Berichtszeitraum bei allen zwölf in Niedersachsen ansässigen Unternehmen erfolgt.

1 22. Tätigkeitsbericht der LfD Niedersachsen 2013-2014: S. 51 ff.

Schwerpunkte der Überprüfung

Jede CR musste eine repräsentative und aktuelle Auswahl ihrer Stichprobenfälle zu den berechtigten Interessen der Auskunftsersuchenden vorlegen. Dabei war/waren auch anzugeben:

- die Kriterien der Fallauswahl,
- die Anzahl der dahinter stehenden Auskunftsfälle,
- der dahinter stehende Auswahlzeitraum,
- die Anzahl der Beanstandungen mit Beanstandungsgründen und
- die daraus im Einzelfall gezogenen Konsequenzen.

Ferner waren folgenden Fragen zu beantworten:

- Kommunikation:
  In welcher Weise informieren die CRen ihre Mitglieder, wozu Stichproben dienen und was hierzu aus hiesiger Sicht erwartet wird (Beantwortungspflicht, Art und Umfang der Beantwortung, Sanktionen für Fälle einer nicht ordnungsgemäßen Beantwortung)?

- Dokumentation:
  In welcher Weise kommen die CRen ihrer Dokumentationspflicht nach?

- Auswertung:
  In welcher Weise analysieren die CRen die Rückantworten auf die Stichprobeanfragen?

- Nachfassen:
  Was veranlassen die CRen, sofern die Antwort auf eine Stichpro-benanfrage nicht ausreichend, nicht vollständig oder gar nicht erfolgt?

- Sanktionen:
  Welche vertraglichen Konsequenzen drohen die CRen an, sofern eine Stichprobenanfrage nicht ordnungsgemäß oder gar nicht beantwortet wird?
  Welche Konsequenzen sind vertraglich vorgesehen, sofern sich bei der Stichprobenüberprüfung zeigt, dass kein berechtigtes Interesse für eine Anfrage bestand?

- Vorformulierte Anfragegründe:
  Welche vorformulierten Anfragegründe nutzen die CRen?
  In welcher Weise werden diese erläutert?

- (Lese-)Zugriff anderer Creditreform-Gesellschaften auf die Auskunfteidaten einer einzelnen niedersächsischen CR:
  In welcher Weise erstreckt eine niedersächsische CR die Stichproben auch auf die (Lese-) Zugriffe anderer Creditreform-Gesellschaften?

Ergebnisse der Überprüfung

Sämtliche überprüften CRen haben fristgerecht und weitgehend vollständig die ihnen gestellten Fragen beantwortet. Angeforderte Unterlagen wurden vorgelegt.

Im Anschluss daran wurde nahezu jede CR im Rahmen einer ergänzenden Vor-Ort-Kontrolle an ihrem Geschäftssitz aufgesucht. Die jeweiligen Prüfergebnisse wurden mit der Geschäftsführung und der/dem jeweiligen Datenschutzbeauftragten erörtert.

Die Prüfungen haben Folgendes ergeben:

Sämtliche niedersächsische CRen informieren ihre CR-Mitglieder, wozu Stichproben dienen und welche Anforderungen an diese nach hiesiger datenschutzrechtlicher Auffassung gestellt werden.

Lediglich wenige Nutzervereinbarungen, die die Voraussetzungen für einen Online-Zugriff eines CR-Mitglieds auf die Datenbank einer niedersächsischen CR regeln, mussten aus Transparenzgründen nachgebessert werden.

Auch die Art und der Umfang der erwarteten Dokumentationen waren im Wesentlichen nicht zu beanstanden. Nur bei wenigen CRen haben aussagekräftige Unterlagen oder Notizen gefehlt, so dass in diesen Fällen eine sachgerechte Nachprüfung für das Vorliegen eines berechtigten Interesses nicht möglich war.
Diese CRen mussten sich deshalb einer ergänzenden Nachprüfung unterziehen.

Einheitlich wird eine repräsentative Stichprobe auf der Grundlage von 2 Promille des Anfragevolumens in einem jeweiligen Stichprobenzeitraum gebildet. Dieser Stichprobenzeitraum entspricht weitgehend einem Monat.

Der gesamte Schriftwechsel wird in Papierform grundsätzlich rückwirkend bis zu einem 1 Jahr archiviert. Anschließend erfolgt nur eine elektronische Speicherung von maximal 3 Jahren.
Nur wenige CRen mussten darauf hingewiesen werden, ihre längeren Aufbewahrungsfristen (von bis zu 4 Jahren) entsprechend anzupassen.

Die Prüfungen haben ferner ergeben, dass sämtliche CRen nach den Vorgaben des Stichprobenkonzepts verfahren. So werden alle Rückantworten dahingehend überprüft, ob sie vollständig und ordnungsgemäß sind.
Hierbei haben die CRen weitgehend darauf geachtet, dass die Antworten auf die Stichprobenanfrage gegenüber der ursprünglichen Angabe des Anfragegrundes in der Online-Maske des Auskunftssystems aussagekräftig ergänzt wurden.
Dies erfolgte entweder durch eine kurze schriftliche Erläuterung oder durch Beifügen von Kopien des zugrunde liegenden Vertrags-/Antragsvorgangs.

Ferner wurden die Rückantworten auch überwiegend daraufhin überprüft, ob der ursprünglich angegebene Abfragegrund tatsächlich mit dem im Rahmen des Stichprobenverfahrens genannten Abfragegrund übereingestimmt hat.

Zweifelsfälle haben die meisten CRen gesondert überprüft und das Prüfergebnis gesondert dokumentiert.

Sämtliche niedersächsische CRen haben in den Fällen, in denen eine Antwort auf eine Stichprobenanfrage nicht ausreichend, nicht vollständig oder gar nicht erfolgt ist, an eine vollständige Beantwortung erinnert.
Dies erfolgte entweder schriftlich oder telefonisch.
Allerdings war vereinzelt festzustellen, dass die CRen nicht ausreichend konsequent nachgehakt haben, bis tatsächlich die erforderliche Antwort vorlag.

Besonders positiv ist hier eine niedersächsische CR aufgefallen: Diese forderte mithilfe sog. Erinnerungs- oder Nachfassschreiben, in denen nochmals ausdrücklich das Stichprobenverfahren erläutert wird, eine Rückantwort bei ihren Mitgliedern an.

Nach dem Stichprobenkonzept kommen als Sanktionen in Betracht:

a) Abmahnung mit Androhung des Ausschlusses vom Auskunftsbezug, der Kündigung der Mitgliedschaft und/oder der Anzeige des Vorganges bei der zuständigen Datenschutzaufsichtsbehörde
b) Ausschluss vom Auskunftsbezug und/oder Kündigung der Mitgliedschaft
c) Anzeige bei der zuständigen Datenschutzaufsichtsbehörde

Sanktionen sind für den Fall, dass eine Stichprobenanfrage nicht oder nicht ordnungsgemäß beantwortet wird, anzudrohen.
Daher sind die von einer CR festgestellten Beanstandungsgründe für Prüfzwecke auch sorgfältig zu dokumentieren.

Sanktionen kommen auch in Betracht, wenn eine Stichprobe zeigt, dass kein berechtigtes Interesse an einer Bonitätsabfrage bestand.

Für den Fall, dass ein CR-Mitglied an seine Beantwortungspflicht erinnert werden muss, wird es auch an die o. g. Sanktionsmöglichkeiten erinnert.

Erfreulicherweise konnte im Rahmen des Prüfverfahrens festgestellt werden, dass nur sehr selten Anlass Bestand, eine Sanktion gegen ein CR-Mitglied auszusprechen.

Allerdings hat eine CR ihr Mitglied konsequenterweise abgemahnt und schließlich mit sofortiger Wirkung vom Auskunftsbezug ausgeschlossen. Dieses CR-Mitglied hatte auch auf das 2. Schreiben, mit dem es an seine Antwort erinnert worden ist, nicht reagiert.

Schließlich wurde im Rahmen der Prüfung bei allen CRen das Thema (Lese-)Zugriff anderer Creditreform-Gesellschaften auf die Auskunfteidaten einer einzelnen niedersächsischen CR erörtert. Dabei vertraten einige CRen zunächst die Auffassung, dass eine stichprobenartige Überprüfung der (Lese-)Zugriffe anderer CR-Gesellschaften verzichtbar sei wegen

- der für alle CR-Mitarbeiterinnen und CR-Mitarbeiter geltenden arbeitsvertraglichen Pflichten sowie
- der Pflicht zur Einhaltung des Datengeheimnisses.

Die Prüfungen wurden zum Anlass genommen, nochmals auf die bereits seit 2012 vertretende Auffassung hinzuweisen, wonach die Stichproben auch auf die (Lese-)Zugriffe anderer CR-Gesell-

schaften zu erstrecken sind. Die CRen sind selbstständig und somit auch als „Dritter“ (§ 3 Abs. 8 Satz 2 BDSG) i. S. von § 29 Abs. 2 Nr. 1 BDSG anzusehen.

Mittlerweile haben sämtliche niedersächsischen CRen ihre Stichprobenprüfungen entsprechend erweitert. Das kann im Wesentlichen auf mein Prüfverfahren zurückgeführt werden.

Fazit

Die niedersächsischen CRen haben gezeigt, dass sie ihre Stichprobenpflicht ernst nehmen. Die Anforderungen des datenschutzkonformen Stichprobenkonzepts von 2012 wurden weitgehend erfüllt.

Nur einige wenige CRen konnten in dieser Hinsicht nicht allen Belangen gerecht werden. Diese haben bisher bereitwillig angekündigt, zukünftig ihr Stichprobenverfahren entsprechend anzupassen. Das wird Gegenstand einer erneuten Nachprüfung durch mich sein.

Ausblick

Die Europäische Datenschutzgrundverordnung (DS-GVO) wird nach der Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam.
In dieser gibt es keine gesonderten Regelungen für Auskunfteien mehr.

Allerdings enthält die DS-GVO abstrakte Regelungen, die auch auf Auskunfteien anzuwenden sind.
Ob und inwieweit sich daraus eine Stichprobenpflicht für Auskunfteien in dem oben beschriebenen Umfang ableiten lässt, ist im Kreise der deutschen Aufsichtsbehörden noch nicht abschließend geklärt.

6.3 Was Immobilienmakler alles wissen wollen - Ergebnisse einer anlassfreien Prüfung -

Die aktuelle Wohnungsknappheit in vielen Regionen Niedersachsens beeinflusst das Verhalten der „Marktteilnehmer" deutlich. So sind Mietinteressenten gegenüber Vermietern und Immobilienmaklern zu fast jeder Auskunft bereit, um sich dem künftigen Vertragspartner als zuverlässiger Mieter mit guter Bonität zu präsentieren. Vermieter und Makler ihrerseits wollen kein Risiko eingehen und möglichst bereits zu Beginn der Mieterauswahl wissen, wer ihnen gegenüber als Mietinteressent auftritt und ob er als geeigneter Mieter in Betracht kommt. Dies führt häufig zum „gläsernen" Mietinteressenten.

Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten" unter https://www.lfd.niedersachsen.de/themen/wirtschaft/mieten_und_wohnen_wohnungswirtschaft/hinweis--undinformationssystemderversicherungswirtschaft-123621.html

Bereits im Jahr 2014 hat sich daher der Düsseldorfer Kreis in einer Orientierungshilfe zu der Frage geäußert, was Vermieter zu welchem Zeitpunkt im Vermietungsprozess fragen dürfen.

Im Rahmen einer anlassfreien Prüfung dazu habe ich mich schwerpunktmäßig mit der Realität befasst.

Dazu habe ich 29 niedersächsische Immobilienmakler befragt, von denen ich auch wissen wollte, wie deren Vorgehensweise im Verkaufsprozess ist.
So war unter anderem Prüfgegenstand, ob und wozu Ausweiskopien gefertigt werden und wie sich die Datensicherheit im Rahmen der elektronischen Kommunikation (Online-Fragebögen, E-Mail-Verkehr, mobile Datenträger) gestaltet.

Lediglich bei einem der geprüften Unternehmen konnten keine Verstöße gegen datenschutzrechtliche Bestimmungen festgestellt werden.

Während es im Verkaufsprozess kaum Beanstandungen hinsichtlich der Fragestellungen an die Interessenten gab, wurden in 13 Fällen die erfragten Daten bzw. der Zeitpunkt der Abfragen im Vermietungsprozess von mir beanstandet.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, soweit das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat (§ 4 Abs. 1 BDSG). Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht (§ 4a Abs. 1 BDSG). Wenn der Abschluss eines Mietvertrages von der Erhebung bestimmter Angaben abhängig gemacht wird, fehlt die Wahlfreiheit des Betroffenen und somit die Freiwilligkeit bei der Einwilligung.

Rechtsgrundlage für die durch den Vermieter verlangten Auskünfte kann daher nur § 28 Abs. 1 Nrn. 1 und 2 BDSG sein.

Die Erhebung, Speicherung, Veränderung oder Übermittlung der personenbezogenen Daten der Mietinteressenten ist für die Erfüllung eigener Geschäftszwecke (des Vermieters) demnach nur dann zulässig gem.

- § 28 Abs. 1 Nr. 1 BDSG, wenn sie zur Begründung eines rechtsgeschäftlichen Schuldverhältnisses (Mietvertrag) mit dem Betroffenen erforderlich ist.
- § 28 Abs. 1 Nr. 2 BDSG, soweit sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Stets unzulässig sind vor diesem Hintergrund die Fragen nach dem Familienstand des Mietinteressenten, der Staatsangehörigkeit, der Beschäftigungsdauer, der etwaigen Befristung des Arbeitsverhältnisses, dem Grund des Wohnungswechsels, bestehenden Rechtsstreitigkeiten, anhängigen Strafverfahren, Hobbies und nach dem Verwandtschaftsgrad und Alter der Mitbewohner. Diese Informationen sind zur Entscheidung über eine Gebrauchsüberlassung nicht erforderlich.
Sofern die Angaben für Ehegatten oder Lebenspartner erfragt wurden, obwohl diese nicht Mietvertragspartei sind, wurden die Fragen aus dem gleichen Grund von mir beanstandet.
Auch die Frage nach Musikinstrumenten kann nur dann für das Mietverhältnis relevant sein, wenn bauliche Besonderheiten Anlass dafür bieten. Ansonsten ist die Nutzung von Musikinstrumenten im Rahmen des Mietvertrages bzw. einer Hausordnung zu regeln.

Oftmals wurden die Kontaktdaten des Arbeitgebers oder des bisherigen Vermieters erfragt. Ergänzend wurden Vorvermieterbescheinigungen angefordert. Diese Vorgehensweise widerspricht dem Grundsatz der Direkterhebung (§ 4 Abs. 2 BDSG), wonach personenbezogene Daten grundsätzlich beim Betroffenen zu erheben sind.

Auch die Vorgehensweise zur Prüfung der Bonität der Mietinteressenten war vielfältig.
Die erbetene Angabe von Zahlungsverpflichtungen, Unterhaltszahlungen, Mahnverfahren, Zahlungsklagen und Insolvenzverfahren bis hin zur Vorlage einer „Schufa"-Selbstauskunft sind dabei ebenso unzulässig wie Fragen nach der eidesstattlichen Versicherung oder frühere Mietschulden für Zeiträume, die alleine schon aufgrund des zeitlichen Abstands zum aktuell angestrebten Mietverhältnis keine Aussagekraft für die Mietzahlungswilligkeit und
-fähigkeit haben.

Grundsätzlich hat der Vermieter zu dem Zeitpunkt der Entscheidung für einen Mietinteressenten die Möglichkeit, die Bonität des konkret ausgewählten Bewerbers zu prüfen. Hierzu darf er Bonitätsauskünfte einer Wirtschaftsauskunftei einholen.
Eine Einwilligung in die Bonitätsabfrage durch den Mietinteressenten ist dazu nicht erforderlich und wäre zudem auch unwirksam. Da der Vertragsabschluss von dem Ergebnis der Bonitätsauskunft abhängig sein kann, ist die erforderliche Freiwilligkeit in die Einwilligung in aller Regel nicht gegeben.

Die Prüfung hat die datenschutzrechtlich problematische Praxis gezeigt, dass die Immobilienmakler umfangreiche Auskünfte von den Mietinteressenten oft bereits zu Beginn des Vermietprozesses verlangen.
So wurden teilweise schon zum Besichtigungstermin Angaben über die Bankverbindung, die Vorlage von Einkommensnachweisen oder auch Name und Anschrift von Bürgschaftsgebern angefragt. Solche detaillierten Informationen müssen zu diesem frühen Zeitpunkt dem Vermieter/Immobilienmakler jedoch noch nicht vorliegen. Auch die Kenntnis der Namen der Mitbewohner ist zu Melderechtszwecken erst bei Abschluss des Mietvertrages erforderlich.

In 14 Fällen wurde die Anfertigung von Ausweiskopien von mir beanstandet.
Nach einem rechtskräftigen Urteil des Verwaltungsgerichts Hannover vom 28.11.2013 (Az.: 10 A 5342/11) stellt das Scannen und Speichern von Personalausweisen einen schwerwiegenden Verstoß gegen die Bestimmungen des Personalausweisgesetzes dar. Das Kopierverbot ist danach aus dem Eigentum des Bundes an Pässen und Personalausweisen sowie indirekt aus § 14 Personalausweisgesetz (PAuswG) ableitbar.
Eine Ausweiskopie ist ausschließlich bei Abschluss eines Makler- oder Kaufvertrages nach dem Geldwäschegesetz (GWG) erforderlich, wenn der Vertragspartner nicht persönlich anwesend ist (§ 6 Abs. 2 Nr. 2 GWG). In allen anderen Fällen ist die Vorlage eines Ausweises zum Abgleich der Angaben ausreichend.

Aufgrund meiner Beanstandungen haben mit einer Ausnahme alle geprüften Immobilienunternehmen umgehend reagiert und überabeitete Konzepte vorgelegt, die die Ergebnisse meiner Prüfung berücksichtigten. Nach weitergehenden Erläuterungen hat aber auch das letzte Unternehmen alle Forderungen umgesetzt.

6.4 Speicherung von Schwarzfahrerdaten datenschutzgerecht gestaltet

Im Berichtszeitraum habe ich eine anlassfreie Kontrolle bei vierzehn niedersächsischen Unternehmen des öffentlichen Personennahverkehrs und des länderübergreifenden schienengebundenen Regionalverkehrs durchgeführt, die die Praxis der Erhebung und Verarbeitung von Fahrgastdaten nach Erheben eines erhöhten Beförderungsentgelts (EBE) zum Gegenstand hatte.

Im Rahmen dieser Kontrolle habe ich u.a. erfragt,

- welche Daten erhoben werden,
- zu welchem Zweck die Datenerhebung und Datenspeicherung stattfindet,
- wie lange die Daten gespeichert werden und
- auf welcher Rechtgrundlage die Erhebung und Verarbeitung der Fahrgastdaten erfolgt.

Tatsächlich haben fast alle befragten Unternehmen Fahrgastdaten im Zusammenhang mit dem EBE erhoben. Lediglich ein Busunternehmen praktiziert die datensparsame und wirtschaftlich sinnvolle Kontrolle der Fahrausweise direkt beim Einstieg. Für schienengebundene Verkehrsmittel ist dies jedoch kaum praktikabel.

Leider fehlte es oftmals sowohl an der Differenzierung der Zwecke und der damit einhergehenden Verpflichtung, die Verwendung der EBE-Daten für andere Zwecke zu sperren.
Auch eine datenschutzrechtliche Rechtsgrundlage konnten mehrere Verkehrsunternehmen zur Legitimierung ihrer Praxis der Kundendatenerhebung und –speicherung nicht nennen.
Tatsächlich ist die Erhebung und Verarbeitung der zur Abwicklung des EBE erforderlichen Fahrgastdaten auf Grundlage des § 28 Abs. 1 Nr. 2 BDSG datenschutzrechtlich im Grundsatz nicht zu beanstanden. Als problematisch hat sich jedoch die von den Verkehrsunternehmen praktizierte Speicherdauer der EBE-Daten erwiesen, die regelmäßig einen Zeitraum von 2-3 Jahren umfasste.

Werden Fahrgastdaten auch erhoben, um Betrug oder das Erschleichen von Beförderungsleistungen zur Anzeige zu bringen, ist zu beachten, dass es sich um Antragsdelikte handelt. Der Antrag auf Strafverfolgung muss in diesen Fällen bis zum Ablauf einer Frist von drei Monaten gestellt werden.
Eine Speicherung der Fahrgastdaten über einen Zeitraum von drei Monaten hinaus wäre abgesehen von einem im Einzelfall ggf. länger als drei Monate dauernden Inkasso des EBE lediglich denkbar, wenn die Beförderungsbedingungen als Vertragsgrundlage genaue Angaben über den Grund und den

Umfang der Datenerhebung und die Speicherfristen enthalten würden und der Fahrgast erkennen kann, in welchen Fällen es im Wiederholungsfall zu einer Strafanzeige kommen wird.
Derartige Regelungen enthielten die Beförderungsbedingungen der geprüften Verkehrsunternehmen jedoch durchweg nicht.
Zudem ist zu berücksichtigen, dass Kinder bis zur Vollendung des 14. Lebensjahres nicht strafmündig sind und eine Speicherung deren Daten zum Zwecke der Strafverfolgung unzulässig ist.
Auch bei sogenannten „Graufahren", also Personen, die einen gültigen Fahrausweis (z.B. Monatskarte) besitzen, den sie aber bei der Kontrolle nicht vorzeigen können, ist eine weitere Speicherung der Daten nach dem nachträglichen Nachweis eines gültigen Fahrausweises und der Entrichtung des dann regelmäßig reduzierten EBE nicht notwendig.

Zu Kritik führte auch der Umfang der im Rahmen des EBE erhobenen Fahrgastdaten. So konnten die Verkehrsunternehmen nicht schlüssig die Erforderlichkeit der Datenerhebung zum Geburtsort des Fahrgastes, zu seiner Nationalität, zur ausstellenden Behörde des Ausweises und zum Gültigkeitsdatum des Ausweises darlegen.

Im Rahmen meiner Prüfung habe ich die Verkehrsunternehmen dazu veranlassen können, den Umfang der Datenerhebung bei EBE-Sachverhalten auf das erforderliche Maß zu beschränken, ihre Beförderungsbedingungen entsprechend anzupassen und vor allem die Speicherdauer der EBE-Daten deutlich zu reduzieren.
Die Beförderungsbedingungen und das intern hinterlegte Verfahren sehen jetzt einheitlich vor, dass die Löschung der „Schwarzfahrerdaten" spätestens ein Jahr nach dem letzten einschlägigen Vorfall erfolgt, um keine unzulässige „Vorratsdatenspeicherung" zu betreiben. Mit dieser Lösung ist es mir gelungen, bei den niedersächsischen Verkehrsunternehmen ein datenschutzgerechtes EBE-Management zu implementieren, das zu einem sachgerechten Ausgleich zwischen den Interessen der betroffenen Fahrgäste und den berechtigten Interessen der Verkehrsunternehmen an einer effektiven Bekämpfung von Beförderungserschleichung führt.

6.5 Funkrauchwarnmelder – Datensammler zur Mieterausforschung?

Bis zum 31.12.2015 mussten in Mietwohnungen Schlafräume und Kinderzimmer sowie Flure, über die Rettungswege von Aufenthaltsräumen führen, nach den Bestimmungen der Niedersächsischen Bauordnung (§ 44 Abs. 5 NBauO) jeweils mit mindestens einem Rauchwarnmelder ausgestattet werden.

Hohe Wellen schlugen während des Berichtszeitraumes daher diverse Spekulationen über den Umfang der von Funkrauchwarnmeldern erhobenen personenbezogenen Daten der Wohnungsnutzer. So wurde behauptet, diese könnten nicht nur Rauch im Fall eines Wohnungsbrandes detektieren. Die Fernauslesefunktion dieser Geräte sei auch nicht darauf beschränkt, deren Funktionsfähigkeit regelmäßig ohne Inanspruchnahme der Mieter prüfen zu können. Vielmehr würden die durch die Geräte erhobenen Daten über den Funktionszustand auch Aussagen über die Nutzung der Mieträume und damit über das Mieterverhalten zulassen. Zudem seien Funkrauchwarnmelder mit versteckten Kameras und Mikrofonen ausgestattet und würden von Vermietern dazu genutzt, um die Mieter in ihrer Privatsphäre auszuforschen.

Daraufhin erreichten mich zahlreiche besorgte Anfragen zur Funktion solcher Geräte und zu der Frage, ob sie datenschutzrechtlich unbedenklich sind.

Anders als einfache Rauchwarnmelder erheben und speichern Funkrauchwarnmelder zu deren Funktionskontrolle Daten, die Veränderungen im und am Gerät und in dessen Umfeld betreffen und die teilweise Auskunft über räumliche Zustände geben. Diese Funktionsdaten, die drahtlos mittels eines externen Lesegerätes von außerhalb der Wohnung ausgelesen werden können, betreffen damit personenbeziehbare sachliche Verhältnisse sind i.S.d. § 3 Abs. 1 BDSG. Die Nutzung von Funkrauchwarnmeldern ist daher datenschutzrelevant.

Sofern keine Einwilligung der Betroffenen (Mieter) i.S.d. § 4a BDSG vorliegt, ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten als Mittel für die Erfüllung von eigenen Geschäftszwecken gem. § 28 Abs. 1 Nr. 2 BDSG nur zulässig, soweit es zur Wahrung der berechtigten Interessen der verantwortliche Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Mit der Installation von Funkrauchwarnmeldern erfüllen Vermieter die bauordnungsrechtlichen Vorgaben. Daher dient deren Einsatz der Wahrung der berechtigten Interessen des Vermieters. Zur Prüfung der Funktionsfähigkeit ist allerdings lediglich die jährliche Auslesung des Ist-Zustandes der Funkrauch-

warnmelder und ggf. ein aggregiertes Ergebnis des Ereignisspeichers erforderlich. Insbesondere die Beschränkung auf ein aggregiertes Ergebnis der gespeicherten Einzelinformationen soll gewährleisten, dass damit ein Verhaltensprofil der Wohnungsnutzer nicht erstellt werden kann. Den schutzwürdigen Interessen der Mieter wird damit angemessen Rechnung getragen.

Diesen Anforderungen werden die von mir geprüften Geräte gerecht. So hat die von mir durchgeführte Prüfung eines Funkrauchwarnmeldesystems, das vor allem von großen Wohnungsunternehmen in Gebäuden mit vielen Mietwohnungen verwendet wird, um die jährliche Funktionsprüfung mit Hilfe der Funkauslesefunktion einfach und für die Mieter komfortabel zu gestalten, insoweit zu keiner datenschutzrechtlichen Beanstandung geführt.
Die Prüfung hat im Übrigen ergeben, dass die Gerüchte um die „Spionage"-Funktion dieser Geräte unzutreffend sind und ins Reich der Legende gehören.

Neben den materiell-rechtlichen Anforderungen an den datenschutzgerechten Einsatz solcher Funkrauchwarnmelder müssen allerdings auch die Formvorschriften aus dem BDSG erfüllt sein. So muss der ein solches Gerät verwendende Vermieter eine Verfahrensbeschreibung (§ 4g i.V.m. § 4e BDSG) erstellen. Sofern er sich zur Durchführung der jährlichen Funktionsprüfung eines Dienstleisters (häufig der Hersteller der Funkrauchwarnmelder) bedienen will, muss der Vermieter zudem mit diesem einen entsprechenden Auftragsdatenverarbeitungsvertrag
i.S.d. § 11 Abs. 2 BDSG abschließen.

6.6 Kurz und knapp – die Teilnehmerliste

Im Zusammenhang mit einer Eingabe wurde ich auf ein Lehrgangs- und Veranstaltungsprogramm aufmerksam, welches gemeinsam von mehreren kommunalen Sportbünden herausgegeben wird. Bei der Anmeldung zu einem der dort angebotenen Lehrgänge erklärte sich die interessierte Person zugleich damit einverstanden, dass die Teilnehmerliste mit Anschrift und Telefonnummer an die übrigen Lehrgangsteilnehmer zur Bildung von Fahrgemeinschaften versendet wird.

Datenschutzrechtlich bedeutet dies, dass die genannten personenbezogenen Daten Anschrift und Telefonnummer durch den Verein bzw. Verband an andere Personen außerhalb der verantwortlichen Stelle übermittelt werden. Dies ist jedoch nur zulässig, wenn eine Vorschrift des Bundesdatenschutzgesetzes oder eine sonstige Rechtsvorschrift dies erlaubt oder soweit der Betroffene eingewilligt hat.
Bei dem hier genannten Zweck der Bildung von Fahrgemeinschaften handelt es sich nicht um einen eigenen Zweck des Sportbundes, so dass sich aus den Vorschriften des BDSG keine Zulässigkeit für eine Übermittlung der personenbezogenen Daten herleiten lässt. Somit bedurfte es hier einer wirksamen schriftlichen Einwilligung durch die betroffenen Lehrgangsteilnehmenden.

Einwilligung nur bei freier Entscheidungsmöglichkeit

Nach § 4a Abs. 1 BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Somit war hier der vorformulierten Erklärung zur Verwendung der personenbezogenen Daten zur Bildung von Fahrgemeinschaften ein Kästchen voranzustellen, durch welches der betroffene Teilnehmende die Einwilligung (Opt-in) mittels eines Kreuzchens im Einzelfall aktiv erteilen kann.Die personenbezogenen Daten sind dabei auf die hierfür erforderlichen Angaben zur Anschrift und Telefonnummer zu beschränken.

Wird das Feld nicht angekreuzt, liegt entsprechend keine Einwilligung vor und zugleich sind die Daten dieses Teilnehmenden nicht auf die Liste zur Bildung von Fahrgemeinschaften zu setzen.

Ich empfahl den Sportbünden aufgrund der o.g. Rechtsvorschrift die Teilnehmenden unter der Einwilligung noch darauf hinzuweisen, dass eine Nichteinwilligung dazu führt, dass die Daten in diesem Fall nicht in eine solche Liste aufgenommen werden, die Nichteinwilligung aber keine Nachteile für die Lehrgangsteilnehmenden bzw. deren Anmeldung hat.

6.7 Datenschutz wahren beim bürgerschaftlichen Engagement

Im Berichtszeitraum habe ich die Datenverarbeitung einer großen gemeinnützigen Nichtregierungsorganisation, welche als eingetragener Verein von Niedersachsen aus deutschlandweit ihre Kampagnen betreibt, in drei verschiedenen Fällen beanstanden müssen.

Allen Fällen gemeinsam war, dass stets ein nicht rechtmäßiger Umgang mit E-Mail-Adressen erfolgte.

Newsletterversand nur bis zur Abbestellung

Im ersten Fall wandte sich eine Petentin an mich, die sich einst in den Newsletter-Verteiler des Vereins eingetragen hatte und diesen mittlerweile mehrfach vergeblich um Löschung ihrer E-Mail-Adresse aus eben jenem Verteiler sowie aller weiteren zu ihrer Person gespeicherten Daten gebeten hatte.

Daraufhin forderte ich den Verein auf, die personenbezogenen Daten der Petentin antragsgemäß zu löschen und mir dies anschließend schriftlich zu bestätigen. Diesem kam der Verein sowohl mir als auch der Petentin gegenüber umgehend nach.

Personenbezogene Daten sind gemäß § 35 Abs. 2 Satz 2 Nr. 1 BDSG zu löschen, wenn ihre Speicherung unzulässig ist.
Dies betrifft auch personenbezogene Daten, deren Speicherung aufgrund einer Einwilligung ursprünglich zulässig war, die Zulässigkeit aber später wegen des Widerrufs der Einwilligung entfallen ist.
So sind z.B. nach Austritt eines Vereinsmitglieds dessen personenbezogene Daten zu löschen. Die Löschung hat unverzüglich nach Erledigung der im Zusammenhang mit dem Austritt anfallenden Formalitäten (z.B. Zahlung von ausstehenden Mitgliedsbeiträgen) zu erfolgen.
Das Führen von Listen ehemaliger Mitglieder oder Unterstützer ist grundsätzlich unzulässig.
Sofern sich unter den zu löschenden Daten jedoch solche befinden, denen gesetzliche, satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen, sind diese gem. § 35 Abs. 3 Nr. 1 BDSG zunächst zu sperren.
Darüber hinaus ist der Versand eines Newsletters zu Werbezwecken insbesondere am Maßstab des Gesetzes gegen den unlauteren Wettbewerb (UWG) zu messen. Hiernach gilt E-Mail-Werbung als unzumutbare Belästigung, sofern nicht die ausdrückliche Einwilligung des Adressaten vorliegt. Dies gilt im Umkehrschluss somit auch im Falle des Widerrufs.

Double-Opt-In als wirksame Einwilligung

Auf den nächsten Fall wurde ich durch den Hinweis eines Zeitungsredakteurs aufmerksam, woraufhin ich bei einem Besuch der Internetseite des Vereins feststellte, dass dieser bei Unterzeichnung eines dort offerierten Appells für eine Kampagne zugleich die Einwilligung des Unterzeichnenden für Informationen über den Fortgang dieser und weitere Aktionen fingierte.
Dies widersprach jedoch dem Zweckbindungsgrundsatz, nachdem ein personenbezogenes Datum nur für den vorher festgelegten Zweck genutzt werden darf.

Hier wurde die Unterzeichnung eines Appells also unzulässigerweise mit der Opt-In-Abfrage in einem (demselben) Schritt (Klick) verbunden.

Nach § 28 Abs. 3 BDSG ist die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung jedoch nur zulässig, soweit der Betroffene eingewilligt hat.
Das gilt insbesondere auch für die Nutzung erhobener E-Mail-Adressen für werbliche Zwecke.
Das Informationsangebot des Vereins, insbesondere hinsichtlich weiterer Aktionen, war als Werbung zu werten.
Somit ist die Einwilligung zum Erhalt weiterer Informationen über den Fortgang dieser und weiterer Aktionen getrennt von dem jeweiligen Appell einzuholen.

Die Einwilligung dient dem Recht auf informationelle Selbstbestimmung und trägt dem Prinzip Rechnung, dass der Einzelne grundsätzlich selbst über die Verwendung seiner personenbezogenen Daten entscheiden kann. Sie ist in § 4a BDSG geregelt und hiernach nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Dieser ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.
Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.
Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

Zudem ist eine solch werbende E-Mail als unzumutbare Belästigung nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) zu werten.

Bei einer Einwilligung auf elektronischem Wege in die Versendung von Newslettern bzw. E-Mail-Werbung bedarf es eines sogenannten „Double-Opt-In". Dabei erteilt die einwilligende Person bei der Anmeldung zum Newsletter o.ä. im ersten Schritt die Einwilligungserklärung durch Angabe der E-Mail-Adresse und zudem meist durch aktives Ankreuzen eines entsprechenden Feldes auf der Internetseite, welches systemseitig nicht bereits vorangekreuzt sein darf.
Im nächsten Schritt sendet der Verein eine kurze E-Mail an die benannte Adresse mit der Bitte, die Einwilligung per Klick auf einen Bestätigungslink endgültig zu verifizieren und freizuschalten.
Mit der Aktivierung dieses Links bestätigt der Inhabende der E-Mail-Adresse die Anmeldung und die Einwilligung zur Verwendung dieser E-Mail-Adresse für den Versand von Newslettern oder weiteren Informationen. Erst wenn dieser Link geklickt und beim Empfänger verarbeitet wurde, ist der Double-Opt-In abgeschlossen und der Newsletter darf versandt werden.
Hintergrund dieses von der Rechtsprechung geforderten Verfahrens ist die Beweisbarkeit der Einwilligung. Da nur der Inhabende des E-Mail-Kontos Zugriff auf die Bestätigungsmail hat, wird auf diese Weise sichergestellt, dass auch nur diese Person die eigene E-Mail-Adresse für den Newsletter freigegeben hat.

s.a. Urteil des BGH vom 16.07.2008 (Az. VIII ZR 348/06)

Der Verein muss als Versender des Newsletters die Bestätigung durch das Double-Opt-In erhalten, um die Einwilligung des Adressaten in ausreichendem Maße beweisen zu können. Ihm obliegt die Darlegungs- und Beweislast.

Nach mehreren persönlichen Gesprächen zur datenschutzkonformen Neugestaltung der Kampagnen im Internet wurde das Verfahren so geändert, dass es nun den o.g. datenschutzrechtlichen Grundsätzen des BDSG entspricht.

Zudem enthält jetzt jeder Newsletter und jede E-Mail-Werbung einen Hinweis, dass die erteilte Einwilligung jederzeit für die Zukunft widerrufen werden kann.
Auch hierfür wurde ein Link installiert, der es den Betroffenen ermöglicht, sich ohne weiteres aus dem E-Mail-Verteiler wieder austragen zu können.

Unzulässige Empfehlungsmails (tell-a-friend)

Nach diesem großen Prüfvorgang erhielt ich eine weitere Eingabe, welche die seitens des Vereins verwendete sogenannte tell-a-friend-Funktion thematisierte.
Diesbezüglich stellte ich fest, dass der Verein zur Verbreitung seiner Kampagnen im Internet auf seiner Webseite eine E-Mail-Empfehlung anbot, bei der jedermann bis zu 50 E-Mail-Adressen Dritter auf einmal eingeben konnte, denen dann ein vereinsseitig vorbereiteter Text zugesandt wurde, mit der werbenden Aufforderung, den jeweiligen Appell zu unterzeichnen.

s. Urteil des BGH kam in seinem anliegenden Urteil vom 12.09.2013 (Az. I ZR 208/12)

Diese Datenerhebung bei Dritten widersprach dem Direkterhebungsgrundsatz. Dieser fordert die Erhebung der Daten beim Betroffenen selbst und gilt auch für die Erhebung zum Zwecke der Werbung. Die Erhebung und Verarbeitung sowie Nutzung der E-Mail-Adressen Dritter mittels der auf der Internetseite des Vereins implementierten „tell a friend"-Funktion war daher unzulässig.
Der BGH hat in einem Urteil eine mittels „tell a friend"-Funktion generierte Empfehlungsmail einer unverlangten Werbemail (Spam) gleichgesetzt.

Somit stellt jede E-Mail, die zumindest mittelbar der Absatzförderung dient, ohne vorherige ausdrückliche Einwilligung eine unzumutbare Belästigung dar und ist grundsätzlich auch nach Maßgabe des UWG unzulässig.

Dabei kommt es für die Einordnung als Werbung nicht darauf an, dass das Versenden der Empfehlungsmails letztlich auf dem Willen eines Dritten beruht. Entscheidend ist vielmehr allein das Ziel, welches der Verein mit dem Zurverfügungstellen der Empfehlungsfunktion auf seiner Internetseite erreichen will, hier Dritte auf den Verein und die von diesem angebotenen Leistungen aufmerksam zu machen. Somit enthalten die auf diese Weise versandten Empfehlungsmails Werbung.
Die Verantwortung für die Zusendung der Empfehlungsmails liegt beim Verein als Betreiber der Internetseite, weil der Versand der Empfehlungsmails auf die gerade zu diesem Zweck vom Verein zur Verfügung gestellte Empfehlungsfunktion zurückgeht, ohne dass vorab Gewissheit darüber besteht, ob die empfangenden Dritten sich damit einverstanden erklärt haben.

Nach ausführlicher Darlegung der Rechtslage, erarbeitete der Verein unter meiner Mitwirkung eine neue Empfehlungsfunktion, welche in der mir vorgestellten Form den datenschutzrechtlichen Anforderungen entspricht. Zudem wurden die unzulässig erhobenen personenbezogenen Daten physikalisch gelöscht, weshalb ich in der Folge das aufsichtsbehördliche Verfahren beenden konnte.

6.8 Fehlerhafte Zusendung eines Kontoauszugs

Ein Kreditinstitut meldete mir eine unrechtmäßige Datenübermittlung und unrechtmäßige Kenntniserlangung von Daten durch Dritte nach § 42a BDSG.

Die Meldung erfolgte unverzüglich innerhalb eines Tages fernmündlich und schriftlich nach drei Tagen. Insoweit war das Meldeverhalten des Instituts vorbildlich.

Der Meldung lag folgender Sachverhalt zugrunde:
Ein Sachbearbeiter der Bank griff auf eine Umzugsdatenbank eines großen Unternehmens aus dem Postbereich zu. Diese Datenbank wird von dem Unternehmen geschäftsmäßig angeboten und von sehr vielen Banken, Versicherungen oder Auskunfteien zur Aktualisierung der eigenen Datenbestände genutzt und in das unternehmenseigene System eingespeist. Aufgrund der Information aus der Datenbank wurde zu einem Bankkunden bzw. dessen Familie ein Umzug gemeldet. Der Sachbearbeiter ging daher von einer entsprechenden Familien-Adressänderung aus und versandte den Kontoauszug eines Geschäftsgirokontos des Bankkunden an die vermeintlich neue Adresse. Nicht bekannt war dem Kreditinstitut, dass der Kunde und seine Ehefrau in Trennung lebten. Es war nur die Ehefrau umgezogen. Durch die Zusendung des Auszuges erhielt die Ehefrau daher unrechtmäßig Kenntnis vom Kontostand ihres Ehemannes.
Ich habe – ebenso wie das Kreditinstitut – diesen Vorgang als meldepflichtig nach § 42a BDSG gesehen, d. h. ein Drohen von schwerwiegenden Beeinträchtigungen für das schutzwürdige Interesse des Ehemannes angenommen, da die besondere Trennungssituation zu berücksichtigen war.

Dieser Fall zeigt, dass ein blindes Vertrauen in die Vollständigkeit fremder Auskunftssysteme recht schnell zu fahrlässigen Datenschutzpannen führen kann. Ich empfehle daher den Unternehmen, sich vor der Übernahme von Daten aus anderen Systemen – wie z.B. Adressdaten – mit dem jeweiligen Kunden in Verbindung zu setzen und so die Richtigkeit zu überprüfen.

6.9 Was ist ein „Code of Conduct“? - 20 Spitzenverbände stellen einen Antrag

„Staatssekretärin Zypries begrüßt Anerkennung einheitlicher Datenschutzvorgaben für Geodaten durch Aufsichtsbehörden“ – so die Schlagzeile einer Pressemitteilung des Bundeswirtschaftsministeriums im Sommer 2015. In jenen Tagen waren bundesweite Verhandlungen zwischen zahlreichen Spitzenverbänden der Wirtschaft und den Datenschutzaufsichtsbehörden zu einem Abschluss gebracht worden.

20 Spitzenverbände schließen sich zusammen

Worum ging es? 20 bundesweite Spitzenverbände (u.a. Bundesverband der Deutschen Industrie; BITKOM; Zentralverband des deutschen Handwerks; Hauptverband des Deutschen Einzelhandels; Gesamtverband der Versicherungswirtschaft etc.) hatten sich in einer gemeinsamen Kommission (Kommission für Geoinformationswirtschaft – GIW-Kommision) zusammengeschlossen. Ziel des Zusammenschlusses war u.a., bundesweite Verhandlungen mit den Datenschutzaufsichtsbehörden zu führen, um einen sogenannten Code of Conduct (Verhaltensregeln) zu erarbeiten.

Zunächst: Was ist ein Code of Conduct? Das ergibt sich aus dem Bundesdatenschutzgesetz, genauer: aus § 38 a BDSG. Hiernach können Spitzenverbände untergesetzliche Richtlinien zur Genehmigung vorlegen, durch welche die Gesetzesregelungen des Bundesdatenschutzgesetzes – branchenbezogen – konkretisiert werden.

Aufgrund der Mischung aus vorgegebenem Gesetzesrahmen und Selbstorganisation spricht man auch von „regulierter Selbstregulierung“. Der Vorteil eines solchen Instruments: Es können untergesetzlich zahlreiche Detailfragen, bezogen auf eine bestimmte Branche, bundesweit zentral geklärt werden.

Konkret: Geodaten

Im Fall der GIW-Kommission ging es um Geodaten. Was versteht man darunter? Geodaten sind alle Daten, die mit einer zusätzlichen Standortinformation verknüpfbar sind; sie bilden die Grundlage für Karten und Pläne. Grundsätzlich können sämtliche Daten mit Geoinformationen ergänzt werden. Den Zugang zu diesen Daten regeln Spezialgesetze wie z.B. die Geodaten-zugangsgesetze des Bundes und der Länder. Der Code of Conduct sollte diese Gesetze nicht ersetzen; er diente vielmehr der Umsetzung und Auslegung dieser Spezialgesetze.

Nachweis datenschutzkonformer Geschäftsprozesse führt zu Akkreditierung

Was war der konkrete Inhalt des Code of Conduct? Er richtete sich an Firmen, die einem der beteiligten Spitzenverbände angehören, und die sich bereiterklärten, ihre Geschäftsprozesse zum Nachweis eines datenschutzkonformen Umgangs mit Geodaten freiwillig akkreditieren zu lassen. Eine erfolgreiche Akkreditierung führte zu einem Beitritt der jeweils geprüften Firma zum Code of Conduct. Durch diese Zugehörigkeit wies die einzelne Firma also nach, dass

der darin geregelte Grundstandard eingehalten wird. Sofern diese Firma dann bei – Geodaten haltenden – Behörden einen Antrag nach den einzelnen Geodatenzugangsgesetzen stellte, konnten diese Behörden die Akkreditierung im Einzelfall berücksichtigen, im Rahmen ihres Ermessens.

Ein Mehrwert für den Datenschutz

Die detailreichen Verhandlungen über die Standards und Verfahrensabläufe des Zertifizierungssystems, in die neben zahlreichen anderen Datenschutzaufsichtsbehörden auch meine Behörde eingebunden war, wurden nach vier Jahren abgeschlossen. Das Instrument des „Code of Conduct" gemäß § 38 a BDSG ist damit übrigens im gesamten Bundesgebiet in 15 Jahren erst zum zweiten Mal zur Anwendung gekommen. Gleichwohl ergibt dieses Instrument in speziellen Konstellationen Sinn – wenn für eine gesamte Branche der Datenschutz im Wege der Selbstorganisation detailorientiert geregelt werden soll.

6.10 Datenschutz im Kfz – Autonomes Fahren wirft Fragen auf

In meinem Tätigkeitsbericht 2013/2014 habe ich über die Entschließung berichtet, die ich mit meinen Kolleginnen und Kollegen auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahr 2014 verabschiedet hatte.[1] Darin hatten wir konkrete Forderungen an die Automobilindustrie gerichtet. Was ist seitdem passiert?

Wo ist das vernetzte Auto datenschutzrechtlich derzeit unterwegs? Wohin geht die Fahrt? Und gibt es beim (Daten-)Verkehr auch Stoppschilder?

Wo ist das vernetzte Auto derzeit unterwegs?

In den vergangenen 2 Jahren habe ich zusammen mit meinen Kolleginnen und Kollegen in den Datenschutzaufsichtsbehörden in Bund und Ländern unsere Entschließung aus dem Jahr 2014 mit Leben gefüllt. Es ist uns von vornherein klar gewesen, dass wir den nächsten Schritt nur im konstruktiven Dialog mit der Industrie gehen können. Es ging darum, zunächst die „Leitplanken" für dieses Zukunftsthema zu bauen. Dieser über einjährige, intensive Dialog fand statt mit einigen anderen Landesdatenschutzbeauftragten, die standortbedingt mit dem Thema befasst sind, sowie der Bundesdatenschutzbeauftragten einerseits und dem Verband der Automobilindustrie andererseits. Hierbei wurde eine gemeinsame Erklärung „Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge"[2] erarbeitet. Dieses gemeinsame Papier stellt die Grundlage des Datenschutzes im Kfz dar. Sie hat deshalb eine so hohe Bedeutung, weil erstmals die abstrakten Grundsätze des Bundesdatenschutzgesetzes zusammen mit der Automobilindustrie für das Produkt Kfz auf eine konkrete Anwendungsebene heruntergebrochen worden sind. Es wurde also ein verbindlicher Standard vereinbart. Alle Datenverarbeitungsvorgänge im Kfz dürfen sich daher nur innerhalb dieser Leitplanken bewegen. Die Bedeutung der „Gemeinsamen Erklärung" sollte daher nicht unterschätzt werden, zumal sie auch auf andere Produkte und Branchen ausstrahlt. Die „Gemeinsame Erklärung" ist somit „Vorreiter" des Datenschutzes in der digitalen Welt, für das Internet der Dinge. Auch der Bundesjustizminister hat die Gemeinsame Erklärung als Vorbild für andere Branchen erwähnt. Zudem ist die Gemeinsame Erklärung mittlerweile ins Englische übersetzt worden, als mögliche „Blaupause" für andere europäische Länder.

Gemeinsame Erklärung „Datenschutzrechtliche Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge" https://www.lfd.niedersachsen.de/download/104132/

Was ist nun also Gegenstand des erarbeiteten Textes? Dreh- und Angelpunkt der „Gemeinsamen Erklärung" ist die Personenbeziehbarkeit: Es ist verbind-

1 22. Tätigkeitsbericht der LfD Niedersachsen 2013-2014: „Datenschutz im Kraftfahrzeug: Gläserne Fahrer im rollenden Rechner": S. 60 ff.

2 https://www.lfd.niedersachsen.de/download/104132/

lich vereinbart, dass die bei der Kfz-Nutzung anfallenden Daten jedenfalls dann personenbezogen im Sinne des Bundesdatenschutzgesetzes sind, wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt. Was heißt das konkret? Es hat entscheidende Bedeutung für die Frage, wem „die Daten gehören".

Die Daten gehören dem Fahrer

Vorweg: Sind die Daten anonymisiert und damit in keiner Weise, auch nicht durch Verknüpfungen, rückverfolgbar, so dürfen sie ohne Einschränkung genutzt werden. Ein Beispiel wären Fehlermeldungen, die vom Hersteller anonymisiert für Statistikzwecke und Produktverbesserungen verwendet werden.

Anders ist es jedoch bei personenbezogenen Daten, die im Zusammenhang mit dem Kfz anfallen. Daten sind dann personenbezogen, wenn sie sich auf eine „bestimmte Person" oder zumindest auf eine „bestimmbare Person" beziehen. Eine Person ist dann „bestimmbar", wenn sie z.B. über die Fahrgestellnummer identifizierbar ist. In diesen Fällen liegen also „personenbezogene Daten" vor. Die „Gemeinsame Erklärung" enthält nun hierzu eine verbindliche, auch seitens der Industrie akzeptierte Aussage: Die Daten „gehören" dem Betroffenen. Auf das Kfz bezogen: Die Daten „gehören" dem Fahrer bzw. Halter des Kfz.

Das ist vor allem wichtig für die vorher oft behauptete Kategorie der „rein technischen Daten": Es ist nun festgehalten, dass es eine angebliche Kategorie von „rein technischen Daten" nicht gibt. Weder die Anzahl der Bremsvorgänge noch der Ölverbrauch – um Beispiele herauszugreifen – sind herrenlose Betriebsdaten. Sie sind schon gar nicht uninteressant. Vielmehr geben sie Auskunft darüber, zu welchem Zeitpunkt (Tagesrhythmus!) ein ermittelbarer konkreter Mensch mit diesem Auto gefahren ist; ob er (durch die Speicherung häufiger Bremsvorgänge) erkennbar in der Stadt oder auf der Autobahn unterwegs ist etc.. Somit könnten mit bereits relativ wenigen Informationen Persönlichkeitsprofile gebildet werden. Indem die „Gemeinsame Erklärung" festhält, dass alle im Fahrzeug anfallenden verknüpfbaren Daten personenbeziehbar sind, ist seitens der Industrie akzeptiert worden, dass diese Fahrdaten nicht zu einem „freien Wirtschaftsgut" werden dürfen.

Weitere Punkte der „Gemeinsamen Erklärung" betreffen beispielsweise das Auskunftsrecht gegenüber dem Hersteller bzw. die Frage der „verantwortlichen Stelle" bei online-Kfz einerseits und offline-Kfz andererseits.

Wohin geht die Fahrt? Und gibt es auch Stoppschilder?

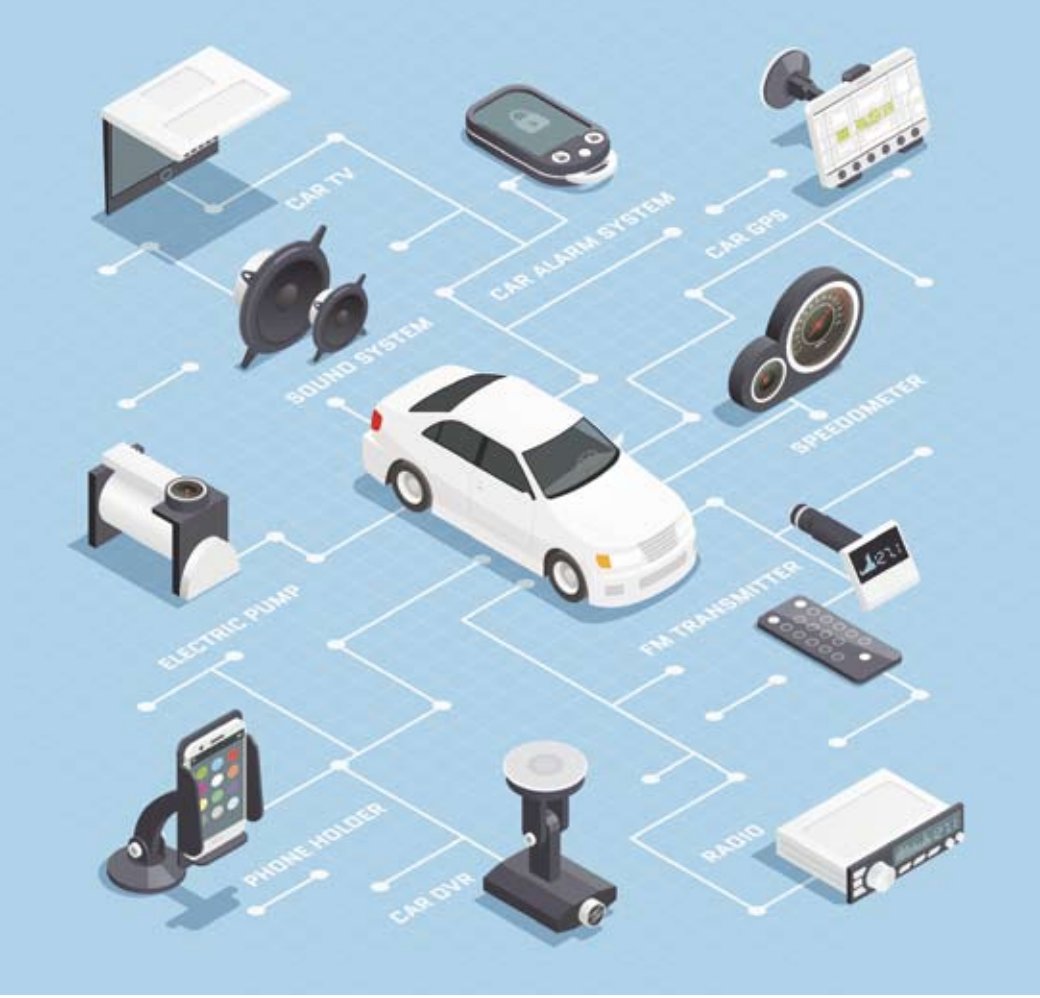
Die rasante Entwicklung des Kfz legt nicht mal einen Tankstopp ein. Wir müssen daher an der Entwicklung „dranbleiben". Zwar ist der Personenbezug der im Auto anfallenden Daten nun verbindlich geklärt. Es bedarf daher für die Datenverwendung einer gesetzlichen Ermächtigung bzw. einer freiwilligen Einwilligung. Diese Regelung zum Personenbezug ist quasi „die Autobahn". Nun gilt es, sich auch um die „Nebenstrecken" zu kümmern. Konkret: Es besteht die Gefahr, dass einzelne Anbieter – infolge der „Gemeinsamen Erklärung" - zwar die Geltung des Datenschutzrechts auch für Betriebsdaten anerkennen, aber künftig den Käufer vor die Alles-oder-nichts-Wahl einer Pauschaleinwilligung stellen. Eine solche Pauschaleinwilligung wäre dann – neben einer gesetzlichen Ermächtigung – eine hinreichende alternative Rechtsgrundlage, sofern sie wirksam ist. Das setzt aber eine freie Entscheidungsmöglichkeit des Käufers voraus.

Ausweichstrecke „Pauschaleinwilligung"

Unzulässiges Ungleichgewicht?

Hier muss ich vielleicht neue Wege beschreiten. Bezieht sich die Wahlfreiheit des Käufers nur darauf, dass er das Auto ja stehenlassen kann bzw. vor dem Kauf darauf verwiesen wird, bei Nichtgefallen eines „Einwilligungspakets" auf den gesamten Autokauf zu verzichten? Oder kommt es darauf an, dass sich der Käufer im Ergebnis einem Anbieter-Oligopol gegenübersieht? Besteht hierbei ein erdrückendes Über-/Unterordnungsverhältnis, also ein unzulässiges Ungleichgewicht? Berücksichtigt man zusätzlich die Besonderheit des Kfz als teilweise „lebensnotwendiges Produkt" und die besondere Eingriffstiefe bestimmter Datenkategorien im Kfz, dann könnte es denkbar sein, bei Vorliegen der entsprechenden rechtlichen Voraussetzungen die Wirksamkeit einer Pauschaleinwilligung zu hinterfragen.

Die Freiwilligkeit der Einwilligung im Über-/Unterordnungsverhältnis ist daher für mich der entscheidende Dreh- und Angelpunkt für den Datenschutz im digitalen Zeitalter. Ich verspreche Ihnen: Wenn nötig, werde ich bei diesem so wichtigen Thema „neue Wege befahren".



6.11 Schwerpunktprüfung bei Inkassounternehmen

Erstmals wurde durch mich eine datenschutzrechtliche Prüfung von Inkassounternehmen durchgeführt

In Niedersachsen waren bisher keine Inkassounternehmen systematisch datenschutzrechtlich kontrolliert worden. Im Berichtszeitraum habe ich nun eine solche Prüfung durchgeführt. Da es eine Vielzahl von Unternehmen unterschiedlicher Größe und Aufgabenstellung gibt und die kleineren überwiegend von Anwaltskanzleien betrieben werden, habe ich bei der Auswahl der zu kontrollierenden Inkassobüros auf die großen, eingeführten Unternehmen abgestellt. Hierbei war auch zu berücksichtigen, dass bei Prüfung von Anwaltskanzleien die Bearbeitung von Inkassofällen häufig auch unter das Mandantengeheimnis fällt und deshalb eine datenschutzrechtliche Kontrolle nur eingeschränkt möglich gewesen wäre.

Somit wurden wegen einer breiteren Betroffenenfrequenz und größerer Organisationsstrukturen sieben Unternehmen in Niedersachsen mit verschiedenen Standorten ausgewählt.

Gegenstand meiner Prüfung war u.a. – bezogen auf den Aufgabenumfang unter datenschutzrechtlichen Aspekten – die Struktur des Unternehmens. Weitere Fragen betrafen die Bestellung des betrieblichen Datenschutzbeauftragten, die interne Datenverarbeitung (Erhebung, Speicherung, Übermittlung und Löschung) und die Wahrung der Betroffenenrechte.

Keine wesentlichen Verstöße festgestellt

Nach Abschluss der Prüfung habe ich keine wesentlichen datenschutzrechtlichen Verstöße festgestellt.

Die von mir geprüften Inkassobetriebe weisen eine unterschiedliche Unternehmensstruktur auf. Sie haben teilweise weniger als 20 Beschäftigte die mit personenbezogenen Daten arbeiten, teilweise über 60 Mitarbeiter.

Sie setzen i.d.R. im Rahmen ihrer Inkassotätigkeit auf dem Markt befindliche elektronische Programme ein, die die datenschutzrechtlichen Anforderungen berücksichtigen. Mit Blick auf die durchgängige Verarbeitung sensibler personenbezogener Daten war den Unternehmen dieser Aspekt besonders wichtig.

Es verblieben daher einige marginale Kritikpunkte. Diese bezogen sich auf die Hinweise, Daten zu sperren, wenn sie nicht mehr zur Abwicklung des Inkassos benötigt werden sowie regelmäßig datenschutzrechtliche Schulungen für Mitarbeiter durchzuführen.

6.12 Schwerpunktprüfung in der Versicherungswirtschaft – Branche ist sich des Schutzes ihrer Kundendaten bewusst

2015 hat meine Behörde eine Prüfung von zehn Versicherungsunternehmen durchgeführt.

Niedersachsen verfügt über rund 50 Versicherungsunternehmen. Einige bieten ein breites, umfassendes Angebot von Versicherungen in verschiedenen Sparten (Lebens-, Kranken-, Sachversicherungen oder Firmenversicherungen) an. Andere Unternehmen haben sich spezialisiert auf Kranken- oder auch Tierversicherungen. Hinzu kommen einige als Anstalt des öffentlichen Rechts organisierte Versicherungen, die überwiegend regional verbreitet sind.

Ende 2015 habe ich eine anlassunabhängige Schwerpunktprüfung der Versicherungsbranche aufgenommen. Die Prüfung der Versicherungsunternehmen diente dem Zweck, sich einen Überblick über die Unternehmensstruktur, die Abläufe innerhalb des Konzerns und die Abläufe innerhalb des Versicherungsunternehmens sowie deren individuelle Stärken und Schwächen zu verschaffen. Ich habe zehn Versicherungsunternehmen mit Hauptsitz in Niedersachsen ausgewählt, die zwischen 200 und 2.500 Mitarbeiter beschäftigten. Die Unternehmen wurden angeschrieben und um Beantwortung von ca. 30 Fragen gebeten.

Die Fragen lassen sich in Fragen zum Unternehmen, zur Konzernzugehörigkeit, zur Organisation, zum Datenschutzbeauftragten und zur Anzahl der Mitarbeiter, in allgemeine Fragen zum Datenschutz und Fragen zur Verarbeitung personenbezogener Daten einteilen.

Branche ist sich Risiken und Schutzansprüchen bewusst

Die Prüfung der einzelnen Stellungnahmen zeigte keine wesentlichen datenschutzrechtlichen Schwächen. Insgesamt ist festzustellen, dass die Versicherungsunternehmen sich des Schutzes ihrer Kundendaten (Versicherungsnehmer/-innen, Geschädigte) und den damit verbundenen Risiken sehr bewusst sind. Noch sensibler erfolgt der Umgang mit besonderen Arten personenbezogener Daten, nämlich den Gesundheitsdaten.

Erwähnenswert sind Feststellungen, die ich bei folgenden zwei Prüfaspekten gemacht habe:
Dabei handelt es sich zum einen um die Dauer der Speicherung der Daten:

Die Versicherungsunternehmen haben zurzeit sehr unterschiedliche Speicherfristen, die – gemessen am Merkmal der Erforderlichkeit – an die gesetzlichen Vorgaben angepasst werden müssen.

So sind Daten u. a. dann zu löschen, mindestens jedoch zu sperren, wenn sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Die Frage der Speicherdauer werde ich noch einmal aufgreifen und einer vertieften Überprüfung unterziehen.

Zum anderen ist die Kommunikation per E-Mail zu nennen:

Die Kommunikation der Versicherungsunternehmen mit Geschäftspartnern, Verbundunternehmen, Versicherungsvermittlern oder Maklern erfolgt häufig über gesicherte Datenleitungen, über einen (beschränkten) Zugang zum System des Unternehmens oder mittels ausreichendem Verschlüsselungsverfahren. Eine solche gesicherte Kommunikation ist datenschutzrechtlich nicht zu beanstanden.

Übermittlung von Gesundheitsdaten darf nur verschlüsselt erfolgen

Bei der Kommunikation der Versicherungsunternehmen mit Versicherungsnehmern oder Geschädigten können allerdings Schwierigkeiten oder Hindernisse auftreten, denn im Privatbereich erfolgt die Verwendung von Verschlüsselungstechniken kaum. Personenbezogene Daten, auch wenn es sich nicht um besondere Arten personenbezogener Daten (z. B. Gesundheitsdaten) handelt, dürfen nur dann mittels E-Mail übermittelt werden, wenn eine Ende-zu-Ende-Verschlüsselung gewährleistet ist. Eine reine Transportverschlüsselung ist regelmäßig nicht ausreichend; das Versicherungsunternehmen kann die Leitungen zwischen den einzelnen Empfängern nicht so kontrollieren, dass die Transportverschlüsselung zwischen Versicherungsunternehmen und jeweiligem Empfänger vollständig sichergestellt wäre.

Ohne eine ausreichende Ende-zu-Ende-Verschlüsslung sollten personenbezogene Daten nur dann mittels E-Mail übermittelt werden, wenn der Kunde diese Kommunikationsart selbst mittels seiner E-Mail eröffnet hat oder er die Antwort ausdrücklich per E-Mail wünscht. Ansonsten können allgemein gehaltene E-Mails mit dem Hinweis auf einen folgenden – postalischen – Schriftverkehr unter Bezug auf datenschutzrechtliche Aspekte erfolgen.

Insgesamt hat die Prüfung der zehn Versicherungsunternehmen datenschutzrechtlich erfreulich wenige Kritikpunkte aufgezeigt. Es handelt sich hierbei um marginale Punkte, die ohne großen Aufwand oder Kosten umgesetzt werden können.

.

6.13 Schwerpunktprüfung Besucher- und Beschäftigtendaten

Im Rahmen einer anlasslosen Schwerpunktprüfung wurde ein Unternehmen geprüft, das im Zusammenhang mit seiner geschäftlichen Tätigkeit und dem Unternehmenszweck mit sehr vielen personenbezogenen Daten in Berührung kommt. Es betreut eine große Anzahl nicht nur aus Niedersachsen stammender Personen, sondern auch internationales Publikum.

Bei der datenschutzrechtlichen Prüfung ging es um die Datenerhebung, -übermittlung und -nutzung sowohl von Besucherdaten als auch von Beschäftigtendaten.

Das schriftliche Kontrollverfahren diente dem Zweck, einen Überblick über die Unternehmensstruktur, die Abläufe innerhalb des Konzerns, die Bestellung des betrieblichen Datenschutzbeauftragten, die interne Datenverarbeitung (Erhebung, Speicherung, Übermittlung und Löschung) sowie die Wahrung der Betroffenenrechte zu erhalten. Dazu wurde ein Fragebogen entwickelt, der auch Fragen zu Kategorien, Herkunft, Weiterleitung Speicherzweck und Löschfristen von Beschäftigtendaten enthielt.

Das Ergebnis der Prüfung zeigte, dass die Übermittlungen von Kundendaten an Tochtergesellschaften bzw. externe Unternehmen rechtmäßig waren. Sie beruhten jeweils auf wirksamen Einwilligungen der Betroffenen. Die Verfahren zur Bestellung (Datenerhebung) und Registrierung sowie die Datennutzung für das Marketing und die Kundenbetreuung boten keinen Anlass zur Kritik. Auch aus dem Bereich der Datenverarbeitung von Beschäftigtendaten ergaben sich keine datenschutzrechtlichen Bedenken.

6.14 Telematiktarif in der Kfz-Versicherung- Beratung eines Versicherungsunternehmens

In der letzten Zeit sind vermehrt Versicherungsunternehmen mit Telematikverträgen oder Telematikanwendungen in Ergänzung zum Kraftfahrzeugversicherungsvertrag auf den Markt gekommen. Diese müssen jedoch strengen Gesetzvorgaben entsprechen.

Klassischerweise errechnet sich im Rahmen eines bisherigen Kraftfahrzeugversicherungsvertrags die Prämie anhand objektiv bestimmbarer Sachverhalte (z. B. nach verursachten Schäden, Wohnort, Automarke und gefahrenen Kilometern). Mit dem Schadenfreiheitsrabatt wird unfallfreies Fahren belohnt. Das Verhalten oder die Fähigkeiten des Fahrers bleiben bei der Tarifierung jedoch außer Betracht.

Im Zuge der vorgesehenen Einführung eines sogenannten Telematikvertrages hat auch mich ein niedersächsisches Versicherungsunternehmen um eine datenschutzrechtliche Beratung gebeten.

Telematik als Ergänzung eines bestehenden Vertrags

Das vom Unternehmen vorgestellte Modell sah vor, dass interessierte Kunden der Kraftfahrzeugversicherung die Möglichkeit erhalten sollten, zusätzlich zum Versicherungsvertrag einen sog. Telematikvertrag abzuschließen. Bei Abschluss des Vertrages erhält der Versicherungsnehmer einen Stecker für eine entsprechende Buchse im Auto.

Telematikanwendungen knüpfen an das Fahrverhalten des Fahrers an. Während der Fahrt werden im Wesentlichen GPS-Daten, Uhrzeit, Fahrzeit, gefahrene Strecke in Relation zur Art der Straße (Autobahn, Land- oder Gemeindestraße), Geschwindigkeit, Beschleunigungs- und Bremsverhalten gemessen und erfasst. Diese Aufzählung ist beliebig erweiterbar, da die Technik kaum Grenzen setzt. Fahrten in der Nacht, insbesondere auch in der Nacht von Samstag auf Sonntag, werden anders bewertet als Tagfahrten. Fahrten über Landstraßen werden anders bewertet als Autobahnfahrten. Plötzliche Bremsmanöver werden ebenso bewertet wie starke Beschleunigungen oder Ausweichmanöver.

Das Versicherungsunternehmen beauftragt in der Regel einen Dienstleister. Dieser bestimmt anhand der erhobenen Fahrdaten und mittels eines vorgegebenen Algorithmus einen Wert, den er dem Versicherungsunternehmen übermittelt. Dieser Wert findet dann im Rahmen der Beitragsrechnung Berücksichtigung. Die erfassten Fahrdaten verbleiben beim Dienstleister, die Versicherung erhält nur den ermittelten Wert.

Die meisten Verträge – so auch die des niedersächsischen Unternehmens – verbinden die Telematikanwendung mit einem Unfallmeldedienst, der dem ab 2018 für Neufahrzeuge gesetzlich vorgeschriebenen e-Call ähnelt und eine beschleunigte Rettung im Falle eines Unfalls auch bei Gebrauchtfahrzeugen gewährleisten soll. Der Unfallmeldedienst ermöglicht Fahrern von Gebrauchtfahrzeugen einen vergleichbaren Rettungsdienst im Notfall, kombiniert mit weiteren Möglichkeiten. Während beim sog. e-Call die Unfalldaten an die Rettungsleitstelle weitergeleitet werden, arbeitet das Versicherungsunternehmen in seiner Telematikanwendung mit eine Meldung an die Versicherung. Erst durch diese wird – abhängig von den Umständen des Einzelfalles und ggfs. auch in Absprache mit dem Fahrer – die Rettungsleitstelle informiert.

Telematikanwendungen sind datenschutzrechtlich nicht grundsätzlich unzulässig, müssen allerdings den strengen Anforderungen des Gesetzes entsprechen. Wesentliche Voraussetzungen für eine datenschutzkonforme Ausgestaltung einer Telematikanwendung sind die Erforderlichkeit der erhobenen Daten, die Datensparsamkeit sowie die Zweckbindung.

Bedeutung im Einzelnen

Personenbezogene Daten dürfen nur insoweit erhoben werden, als sie für die Durchführung der Telematikanwendung bzw. des Telematikvertrages erforderlich sind. Dabei dürfen die erhobenen Daten nur für die Dauer des Zeitraums gespeichert werden, wie sie für die ordnungsgemäße Durchführung des Vertrages erforderlich sind.
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Soweit der Verwendungszweck dies ermöglicht und zulässt, sind personenbezogene Daten zu pseudonymisieren oder zu anonymisieren.

Die an diesen Vorgaben ausgerichtete Beratung des Unternehmens hat insgesamt zum Ergebnis geführt, dass die datenschutzrechtlichen Anforderungen im Wesentlichen erfüllt worden sind. Ich konnte das Unternehmen von einigen Verbesserungsvorschlägen überzeugen. Letztlich wäre zwar eine noch verständlichere und transparentere Einwilligung auch denkbar gewesen. Eine rechtlich zwingende Notwendigkeit hierfür habe ich aber nicht feststellen können.

Einem Versicherungsnehmer, der ein solches Telematikangebot annimmt, muss allerdings bewusst sein, dass er damit einen Teil der Privatsphäre aufgibt. Dies gilt auch für Gastfahrer, die das Kraftfahrzeug nutzen, selbst aber nicht Vertragspartner des Versicherungsunternehmens sind und deren Daten damit ohne entsprechende Grundlage erhoben werden. Eine gesetzliche Zulässigkeit der Erfassung, Speicherung und Nutzung personenbezogener Daten im Rahmen des geschlossenen Vertrages gilt für diese nicht. Es reicht nicht aus, dass ein Gastfahrer Kenntnis von der Telematikanwendung hat, er muss auch einwilligen. Dies kann formlos erfolgen, indem der Gastfahrer vor Fahrtantritt deutlich auf die Telematikanwendung (z. B. gut sichtbarer Aufkleber) hingewiesen wird, so dass er die Möglichkeit hat, das Kraftfahrzeug stehen zu lassen. Bei einigen Modellen ist es auch möglich, die Anwendung ohne großen Aufwand auszuschalten.

Es ist daher ratsam, sich vor Abschluss eines entsprechenden Vertrages nicht nur mit den finanziellen Vorteilen des Telematikmodells sondern auch mit den Details zu befassen. Unerlässlich ist es, dass der Versicherungsnehmer sich genau informiert, welche Daten für welchen Zweck über welchen Zeitraum erfasst, gespeichert und genutzt werden.

6.15 „Datenschutzauskunft“ bedeutet nicht Herausgabe von Unterlagen

Ein Petent wandte sich mit der Frage nach einer Herausgabe von Unterlagen an mich. Dazu schilderte er zwei Sachverhalte: In einem Fall hatte er als Versicherungsnehmer seiner Kraftfahrzeugversicherung einen Schaden an fremdem Eigentum angezeigt, in einem zweiten Fall wurde er als Verursacher eines Schadens ermittelt, den seine Kraftfahrzeugversicherung in der Folge beglichen hat.

Im ersten Fall beantragte der Petent von seiner Kraftfahrzeugversicherung die Herausgabe von Unterlagen, insbesondere des Gutachtens sowie des Kostenvoranschlages des beschädigten Fahrzeuges. Die Übersendung der durch den Gutachter angefertigten Fotos des Schadens reichten ihm nicht aus.

Im zweiten Fall begehrte der Petent von der Kraftfahrzeugversicherung die von dem Geschädigten eingereichten Reparaturrechnungen.
Die Versicherung stellte ihm schließlich Unterlagen zur Verfügung, in denen die personenbezogenen Daten der Geschädigten geschwärzt worden waren. Eine Übersendung von Dokumenten in geschwärzter Form begegnet zwar keinen datenschutzrechtlichen Bedenken, dem Petenten genügte das jedoch nicht. Er verlangte weiterhin die Übersendung der ungeschwärzten Unterlagen.

Daten Dritter dürfen nicht von Versicherungen übermittelt werden

Die vom Petenten gewünschten Unterlagen enthalten personenbezogene Daten Dritter (der Geschädigten), die dem Petenten nicht bekannt sind und aus diesem Grunde auch nicht übermittelt werden dürfen. Übermittelt eine verantwortliche Stelle ohne Rechtsgrundlage oder ohne Einwilligung des Betroffenen (hier: der Geschädigten) die personenbezogenen Daten einem Dritten (hier: dem Petenten), würde sie gegen datenschutzrechtliche Bestimmungen verstoßen.

Das Bundesdatenschutzgesetz (BDSG) regelt die datenschutzrechtlichen Rechte des Betroffenen in den §§ 33 – 35 BDSG:

§ 33 BDSG – Benachrichtigung des Betroffenen – regelt die Pflichten der verantwortlichen Stelle zur Benachrichtigung des Betroffenen, wenn ohne dessen Kenntnis erstmals personenbezogene Daten für eigene Zwecke der verantwortlichen Stelle gespeichert werden.

§ 34 BDSG – Auskunft an den Betroffenen – sieht einen Auskunftsanspruch des Betroffenen gegenüber der verantwortlichen Stelle über die zu seiner Person gespeicherten Daten, deren Herkunft und deren Empfänger sowie den Zweck der Speicherung vor.

§ 35 BDSG – Berichtigung, Löschung und Sperrung von Daten – regelt Ansprüche auf Berichtigung unrichtiger personenbezogener Daten, die Löschung oder Sperrung der Daten.

Ein datenschutzrechtlicher Herausgabeanspruch des Petenten besteht hiernach nicht. Mangels einer entsprechenden Rechtsgrundlage zur Herausgabe von Dokumenten im BDSG ist die Entscheidung der Versicherung datenschutzrechtlich nicht zu beanstanden.

Unabhängig davon bleibt es dem Petenten unbenommen, die Herausgabe der Dokumente auf dem Zivilrechtsweg zu verfolgen.

6.16 Unberechtigter Zugriff auf ein Online-Konto

Durch zu „schwach" gewählte Zugangsdaten eines Bankkunden gelang einem anderen Kunden ein Kontozugriff.

Dem Kundenservice einer Bank wurde folgender Vorfall aus dem Bereich des Online-Banking gemeldet: Ein Kunde wollte sich mittels eines Online-Zugriffs auf sein Konto einloggen und gab hierfür wie gewohnt seine 5-stellige PIN ein. Versehentlich wählte er jedoch als zusätzliche Benutzeridentifikation anstelle seiner Kontonummer seinen Nachnamen. Zu seiner Überraschung gelangte er damit auf das Konto eines anderen Kunden. Dessen Vorname und gewählte PIN waren mit seinen Nutzerdaten identisch.

Der überraschte Kunde, der plötzlich lesenden Zugriff auf die Kontoinformationen und -umsätze des betroffenen Kunden erhalten hatte, meldete diesen Vorfall selbst der Bank. Diese sperrte sofort den Zugang des „ausgespähten" betroffenen Kunden.

Eine Möglichkeit zur Ausführung von Zahlungstransaktionen bestand für den Kunden nicht, denn für eine Zahlungsautorisierung wäre die Eingabe einer TAN notwendig gewesen.

Der unabsichtliche Lesezugriff auf die Kontodaten des betroffenen Kunden konnte nur aufgrund der jeweils schwach gewählten Authentifizierung erfolgen. Die Bank sah hierin kein ihr vorwerfbares Handeln und nahm auch keine Meldepflicht im Sinne des § 42a BDSG an. Diese Auffassung habe ich geteilt.

Dieser Fall zeigt, dass es auch in der Verantwortung des Kunden liegt, hinreichend individualisierte „starke" Benutzernamen zu wählen, damit ein solch unberechtigtes „Mitlesen" gar nicht erst vorkommen kann.

7. Beschäftigtendatenschutz

7.1 E-Mail- und Internet am Arbeitsplatz – was ist erlaubt?

Eine Orientierungshilfe der Datenschutzaufsichtsbehörden gibt Antwort

Am Arbeitsplatz verbringt man einen großen Teil des Tages. Für viele Beschäftigte stellt sich daher die Frage: Darf am Arbeitsplatz auch privat das Internet genutzt werden? Dürfen am Arbeitsplatz private Mails versendet werden? Für den Arbeitgeber stellen sich ähnliche Fragen: Darf auf das E-Mail-Postfach der einzelnen Beschäftigten zugegriffen werden bei einer ungeplanten Abwesenheit? Darf die Internetnutzung kontrolliert werden? Und welche Gestaltungsmöglichkeiten gibt es im Voraus?
Hierzu habe ich zusammen mit meinen Kolleginnen und Kollegen der Datenschutzaufsichtsbehörden der Länder und des Bundes im Berichtszeitraum eine Orientierungshilfe erstellt. Zeitweise war hierbei meine Behörde federführend. Die Orientierungshilfe versucht, auf über 30 Seiten das Thema umfassend darzustellen.
An dieser Stelle soll der Inhalt der Orientierungshilfe in ihren wesentlichen Eckpunkten dargestellt werden.

Was ist, wenn keine Regelung existiert?

Bei diesem Thema ist stets die Vorfrage zu klären, ob den Beschäftigten die private Nutzung des Internets bzw. des betrieblichen E-Mail-Postfachs gestattet ist. Hierbei ist es so, dass eine solche Privatnutzung den Beschäftigten – sofern keine Regelung existiert – erst einmal grundsätzlich verboten ist. Schließlich stellt der Arbeitgeber die Hard- und Software zur Verfügung und bezahlt für die Tätigkeit am Arbeitsplatz. Sofern also keine Regelung existiert, ist eine Privatnutzung untersagt. Erst wenn der Arbeitgeber im Arbeitsvertrag oder in einer Betriebsvereinbarung eine Privatnutzung ausdrücklich gestattet, ist diese erlaubt. Allerdings ist es nach überwiegender Auffassung auch möglich, dass der Arbeitgeber über einen längeren Zeitraum durch Kenntnis und Duldung die private Nutzung konkludent genehmigt (sogenannte „betriebliche Übung“).
Es steht übrigens in der freien Entscheidung des Arbeitgebers, ob er eine Privatnutzung gestattet.

Das rein betriebliche „Surfen“

Wenn also die private Nutzung des Internets nicht erlaubt wurde, kann nur zu betrieblichen Zwecken „gesurft“ werden. Der Arbeitgeber darf dies stichpro-

benartig kontrollieren, allerdings grundsätzlich nur in einem Stufenverhältnis: Zunächst ist es zulässig und ausreichend, wenn er für diesen Zweck nur eine Auswertung des Surfverhaltens ohne Personenbezug vornimmt, insbesondere ohne Einbeziehung der IP-Adresse etc. Eine personenbezogene Vollkontrolle durch den Arbeitgeber stellt dagegen einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar; eine solche personenbezogene Überwachung wäre nur bei konkretem Missbrauchsverdacht im verhältnismäßigen Rahmen zulässig. Hierzu gibt § 32 Abs. 1 Satz 2 Bundesdatenschutzgesetz unter anderem vor, dass zur Aufdeckung von Straftaten personenbezogene Daten der Beschäftigten erhoben und genutzt werden dürfen, wenn dokumentierte tatsächliche Anhaltspunkte den Verdacht begründen, dass die Betroffenen im Beschäftigungsverhältnis eine Straftat begangen haben. Zudem darf das schutzwürdige Interesse des Betroffenen, bei der Abwägung von Art und Ausmaß der Überwachung, nicht unverhältnismäßig sein.

Und was gilt für E-Mail-Accounts, wenn nur die betriebliche Nutzung erlaubt ist? Bei rein betrieblich erlaubter Nutzung darf der Arbeitgeber die einzelnen Mails – wie einen Papiervorgang – zur Kenntnis nehmen. Er darf auch verfügen, dass zum Beispiel zu einem bestimmten Geschäftsvorgang ihm ein- oder ausgehende Mails zur Kenntnis zugeleitet werden. Allerdings wäre eine automatische permanente Weiterleitung sämtlicher ein- oder ausgehenden Mails an Vorgesetzte – sofern nicht arbeitsrechtlich statthaft – auch datenschutzrechtlich mangels Erforderlichkeit unzulässig (sogenanntes Verbot der permanenten Kontrolle).

Die rein betriebliche E-Mail-Nutzung

Für den Fall der Abwesenheit von Beschäftigten sollte der Arbeitgeber ein Stufenmodell anwenden: Primär sollte ein reiner Abwesenheitsassistent, also eine automatisierte Abwesenheitsnachricht, erfolgen. Sofern dies den konkreten betrieblichen Erfordernissen nicht genügt, kann eine Mail-Weiterleitung an einen Vertreter im Vorfeld der Abwesenheit eingestellt werden. Als „letzte Stufe" darf der Arbeitgeber auf bereits empfangene bzw. bereits versandte betriebliche E-Mails zugreifen, allerdings nur unter der Voraussetzung, dass dies für konkrete betriebliche Zwecke – in nachvollziehbarer Weise – zwingend erforderlich ist.

Was gilt im Einzelnen, wenn das private Surfen erlaubt ist?

Das erlaubte private Surfen…

Dann wird der Arbeitgeber zum Telekommunikationsanbieter; er ist daher zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ein Zugriff auf die Protokolldaten (insbesondere: welche Internetseiten einzelne Beschäftigte abgerufen haben) darf der Arbeitgeber daher grundsätzlich nur mit Einwilligung der betreffenden Beschäftigten vornehmen. Der Arbeitgeber kann jedoch die Erlaubnis zu einer Privatnutzung an Bedingungen knüpfen. Insbesondere kann er den zeitlichen Umfang oder auch inhaltliche Verhaltensregeln vorgeben. Vor allem aber kann der Arbeitgeber die Erlaubnis zur Privatnutzung an die Bedingung knüpfen, dass sich die einzelnen Beschäftigten mit Zugriffen und Kontrollen des Arbeitgebers einverstanden erklären. Die Grundzüge hierzu sollten in einer Betriebsvereinbarung geregelt werden. Auf der Grundlage einer solchen Betriebsvereinbarung würden sodann die individuellen Einwilligungserklärungen der Beschäftigten eingeholt werden.

Die Beschäftigten können übrigens ihre Zustimmung zur angebotenen Privatnutzung mit den damit verbundenen Kontrollmöglichkeiten auch verweigern, und zwar ohne arbeitsrechtlichen Nachteil. Dann ist allerdings eine Privatnutzung auch nicht erlaubt, vielmehr gilt dann für sie die Rechtslage wie bei der rein betrieblich erlaubten Nutzung.

… und die erlaubte private Mailnutzung

Auch bei erlaubter privater *E-Mail-Nutzung* ist der Arbeitgeber zur Wahrung des Fernmeldegeheimnisses verpflichtet. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist dem Arbeitgeber grundsätzlich nur mit Einwilligung der betreffenden Beschäftigten gestattet. Der Arbeitgeber sollte daher – sofern er einen solchen Zugriff möchte – auch bezüglich der E-Mails die Erlaubnis zur Privatnutzung an die Bedingung knüpfen, dass sich die einzelnen Beschäftigten mit Zugriffen und Kontrollen des Arbeitgebers einverstanden erklären. Derartige Zugriffe und Kontrollen müssen selbstredend erforderlich und verhältnismäßig sein.

Es ist nochmals zu betonen: Ein Zugriff auf das E-Mail-Postfach der betroffenen Beschäftigten, gerade bei ungeplanter Abwesenheit, ist auch bei betrieblicher Erforderlichkeit in diesen Fällen nur mit der vorab eingeholten Einwilligung dieser Beschäftigten erlaubt. Bei erlaubter Privatnutzung sollte der Arbeitgeber daher ein erhebliches Interesse daran haben, etwaige Fragen im Vorfeld zu klären. Hierfür bietet sich wiederum eine Betriebsvereinbarung an.

Muster-Betriebsvereinbarung

In unserer Orientierungshilfe haben wir eine Muster-Betriebsvereinbarung erstellt. Die Muster-Betriebsvereinbarung und die Orientierungshilfe können auf der Website meiner Behörde heruntergeladen werden.[1]

1 https://www.lfd.niedersachsen.de/themen/wirtschaft/arbeitnehmer/internet_email/internet-und-e-mail-am-arbeitsplatz-146073.html

7.2 Schwerpunktprüfung „GPS“ im Beschäftigtenverhältnis

Beschäftigte sollten während ihrer Arbeitszeit die Möglichkeit haben, sich frei bewegen und unbeobachtet kommunizieren zu können. Zunehmend erreichen mich jedoch Petitionen von Arbeitnehmerinnen und Arbeitnehmern, die mit technischen Hilfsmitteln überwacht werden.

Besonders attraktiv aus Sicht von Arbeitgebern scheint hierbei die geo-bezogene Ortung von Beschäftigten zu sein. Mit Hilfe von Technologien wie GPS (Global Positioning System) oder Handy-Standortlokalisation sind immer exaktere Positionsbestimmungen möglich. Mittels Verwendung von Netzinformationen zu Funkzellen und Verbindungsqualitäten kann ein Handy-Benutzer auch ohne nutzeraktivierte Telekommunikationsverbindungen relativ genau geortet werden. Die Verknüpfung von Positionsdaten mit den personenbezogenen Daten der nutzenden Person ermöglicht die Erstellung von Bewegungsprofilen der Beschäftigten.

a) Als besonders „dynamisch“ erweist sich hierbei der Bereich der Wirtschaft: GPS in der Wirtschaft

Noch vor einigen Jahren waren GPS-Systeme aufwändig und teuer; sie wurden in Branchen eingeführt, die ein solches System tatsächlich zur spontanen Disposition, z.B. ihrer LKW-Flotten, benötigten. Die Digitalisierung schreitet jedoch enorm schnell voran. Innerhalb von ca. drei Jahren wurde GPS plötzlich auch von Branchen eingesetzt, deren LKW-Flotten einem vorher festgelegten Tourenplan folgten (z.B. festgelegte Europatouren) bzw. bei Beschäftigten, die bis dahin ihre Fahrtrouten selbständig entscheiden konnten (z.B. Handelsvertreter).

Auch eine weitere Entwicklung war feststellbar: Neben dem „reinen“ geografischen Standortsignal („klassisches GPS“) wurden zunehmend Zusatzdaten erhoben, gespeichert und übertragen. Als Beispiel sind die Daten „Motor an/aus“; Drehzahlmesser, Fahrzeuggeschwindigkeit und die Temperatur am Auspuff zu nennen.

So ist es keine Fiktion, sondern oft Alltag, dass ein LKW-Fahrer, der auf seiner Fahrt in Spanien im Stau steht, von seinem Chef angerufen wird mit der Frage, warum der Motor aus sei. Zudem werden GPS-Systeme zunehmend auch in Baggern und sogar in Stahlträgern als Diebstahlsschutz eingebaut. Zugleich sind diese GPS-Signale oft permanent aktiviert, so dass die Arbeitsgeschwindigkeit eines Baggers oder die Position des LKW, der die Stahlträger transportiert, zur verdeckten Leistungs- und Verhaltenskontrolle „aus der Ferne“ verwendet werden können.

In einem Beratungsfall ging es sogar um einen Hausmeister, der nur „fußläufig“ in einem Gebäudekomplex seinen Dienst leistete, aber hierbei über sein Diensthandy mittels GPS-Funktion vom Arbeitgeber permanent überwacht wurde. GPS-Überwachung setzt daher nicht mehr unbedingt ein Fahrzeug voraus!

Zu erwähnen ist auch, dass die Auswertungsmöglichkeiten zahlreicher werden. Beispielsweise können von einem bestimmten Fahrzeug „Wochendiagramme“ bzw. Kartenausdrucke mit „optimaler und gewählter Fahrtroute“ ausgedruckt werden. Natürlich ist es auch möglich, dass der Chef am heimischen Arbeitsplatz Fahrtroute und Fahrtverhalten „live“ verfolgt.

Hier setzt der Beschäftigtendatenschutz an. Gerade in der Über-/Unterordnung des Arbeitsverhältnisses führt ein unnötiges GPS-System zu einem unzumutbaren Überwachungsdruck, dem sich die Beschäftigten nicht entziehen können. Vielmehr ist eine solche Datenerhebung bei Beschäftigten gemäß § 32 Bundesdatenschutzgesetz nur zulässig, wenn diese Daten erforderlich sind zur Durchführung des konkreten Beschäftigungsverhältnisses. Bezogen auf GPS-Systeme: Der Einsatz eines solchen Systems und die hierbei konkret erhobenen Positions- und Zusatzdaten müssen tatsächlich erforderlich sein für den individuellen Einsatz der Beschäftigten bzw. zur Erfüllung ihrer Arbeitsaufgabe.

Im Bereich der Wirtschaft habe ich im Berichtszeitraum anlassunabhängig eine Schwerpunktprüfung zum Thema „GPS“ durchgeführt. Hierzu habe ich zwölf niedersächsische Firmen kontrolliert, in Hinblick auf die Erhebung und Verarbeitung von Standortdaten der Beschäftigten. Die Prüfung erfolgte branchenübergreifend. Konkret wurden zwei Bauunternehmen, vier Speditionen und sechs Taxenunternehmen ausgewählt. Die etwaige Verwendung von Positionsdaten wurde jeweils mit 20 Fragen geprüft. Auf diesem Weg habe ich u.a. die Möglichkeit zur Positionsbestimmung, den Zweck einer etwaigen Erhebung, die Häufigkeit, die Übertragungswege, die Datenarten sowie Fragen zur Speicherungsdauer, Zugriffskonzept, Auswertungsmöglichkeiten und Transparenz kontrolliert. Für die rechtliche Bewertung kam es auch darauf an, ob neben der beruflichen Nutzung auch die Privatnutzung von dienstlichen Fahrzeugen erlaubt ist.

Bereich der Verwaltung

Es ergab sich folgendes Ergebnis: Bei fünf der geprüften Unternehmen wird im Beschäftigtenverhältnis kein GPS-System eingesetzt. Sieben der Unternehmen verwenden Systeme zur Positionsbestimmung. Diese Unternehmen wurden über den Prüfzeitraum zu weiteren Stellungnahmen aufgefordert. Im Ergebnis waren bei drei dieser Unternehmen keine datenschutzrechtlichen Verstöße festzustellen. Bei den verbleibenden vier Unternehmen warf die Schwerpunktprüfung – bezogen auf das Konzept der einzelnen Firma – derart vertiefte Fragen auf, dass diese nur in einem individuellen Kontrollverfahren abschließend geklärt werden können.

Als Ergebnis der Schwerpunktprüfung kann daher Folgendes festgehalten werden: Immerhin ein Drittel der geprüften Unternehmen setzt Systeme zur GPS-Bestimmung ihrer Beschäftigten ein, deren Notwendigkeit hinsichtlich Detailgrad, Speicherdauer und Verwendungszweck kritisch hinterfragt werden muss.

b) Im Bereich der Verwaltung habe ich im Berichtszeitraum vier oberste Landesbehörden um Stellungnahme gebeten, ob in ihrem nachgeordneten Geschäftsbereich automatisierte Verfahren zur Standortbestimmung der Beschäftigten eingesetzt werden, die dazu geeignet sind, diese zu überwachen und deren Arbeitsverhalten zu bewerten.

Die stichprobenhafte Abfrage hat gezeigt, dass es keine zeitlich unbefristeten Vollkontrollen gibt, wo sich Mitarbeiterinnen oder Mitarbeiter mit ihrem Dienstwagen oder Handy etc. gerade befinden. Sogenannte „Emergency-Apps" zur Ermittlung von Standortdaten von Beschäftigten kommen nicht zum Einsatz.

Gleichwohl werden im Landesbereich in Zusammenhang mit der Nutzung mobiler IKT-Endgeräte (z. B. Smartphones, Tablets, GPS-Geräte) diverse Verfahren zur Standortbestimmung eingesetzt. Als Zweckbestimmung wurde u. a. angegeben

- Orientierung im Gelände und zum Routing (Einsatz sog. „Tracking-Apps"),
- Notruf bzw. Unfall-Meldung an die Rettungsleitstellen,
- Gerichtsfeste Dokumentation von Einsätzen (z. B. Winterdienstberichte),
- Standortbestimmung von Objekten (u. a. im Bereich Vermessung),
- Lokalisierungsfunktion bei Verlust von Endgeräten (Mobile Device Management -MDM-).

Daneben werden anonymisierte Daten zu Statistikzwecken, für Maßnahmen der Aus- und Fortbildung oder zur Optimierung von Arbeitsabläufen verwendet. Insbesondere in den Fällen, in denen Beschäftigte die Aktivierung der Verfahren nicht selbst steuern können (s. Beispiel „Notruf" oder „MDM"), sorgen Verfahrensbeschreibungen und Dienstvereinbarungen nach § 78 Niedersächsisches Personalvertretungsgesetz mit eindeutigen Festlegungen zu Art und Weise und Umfang der Datenverarbeitungen sowie zu Zweck- und Nutzungsbedingungen für die erforderliche Transparenz bei den betroffenen Beschäftigten. Gegen diese Vorgehensweise habe ich keine datenschutzrechtlichen Bedenken.

Fazit

c) Als Fazit ist Folgendes festzuhalten: Namentlich im Bereich der Wirtschaft nimmt der Überwachungsdruck auf Beschäftigte durch technische Systeme, gerade in Hinblick auf Detailgrad und Datenarten, branchenübergreifend zu. Ich werde dieses für die Beschäftigten sehr wichtige Thema weiter verfolgen.

7.3 Unterliegen Sie dem Mutterschutzgesetz?

Hinweise zur problematischen Fragen in Bewerberbögen

Dass Unternehmen ein großes Interesse an ihren Mitarbeiterinnen und Mitarbeitern haben ist nicht neu. Bei Gesundheitsmanagement, Zielvereinbarungen, Fortbildungen, modernen Arbeitszeitmodellen u.ä. lässt sich meist verhältnismäßig leicht ein Ausgleich zwischen Datenschutz und berechtigten betrieblichen Interessen herstellen. Ein solcher Ausgleich gelingt hingegen nicht, wenn besonders interessierte Personalabteilungen umfangreiche Fragenkataloge an Bewerberinnen und Bewerber versenden.

Wer sich Hoffnungen auf einen neuen Arbeitsplatz macht, wird möglichst alle Fragen beantworten, um im Bewerbungsverfahren weiterhin berücksichtigt zu werden.

Rechtliche Grundlage

Soweit es zur Begründung eines Beschäftigtenverhältnisses erforderlich ist, darf ein Unternehmen personenbezogene Daten von Bewerberinnen und Bewerbern erheben und auch verarbeiten (§ 32 Abs. 1 Satz 1 BDSG).

Seine Grenzen findet diese Ermächtigung, wenn die personenbezogenen Daten objektiv nicht mehr notwendig sind, um über die Einstellung zu entscheiden. Auch wenn die Daten zur Diskriminierung genutzt werden können, sind Erhebung und Verarbeitung nicht erforderlich.

Problematische Fragen

Mir wurde ein Bewerberbogen vorgelegt, der von großer Kreativität zeugte. Unter anderem wollte das Unternehmen Vorname, Beruf, Geburtsdatum und Arbeitgeber des Ehepartners wissen. Auch recht detaillierte Fragen zur Krankengeschichte der letzten zehn Jahre dürften für die Mehrzahl der Arbeitsplätze nicht relevant sein.

Fragen zu Geburtsdatum und -ort, zur Ausweisnummer, zum aktuellen Gehalt, zur Krankenkasse und zu Kindern unter 18 Jahren wirkten im Vergleich noch harmlos. Ähnlich wie die Bitte ein Lichtbild einzukleben und das Datum der Aufnahme anzugeben. Interessant aber, wie das Unternehmen die unzulässige Frage nach einer Schwangerschaft umschiffte: *„Unterliegen Sie dem Mutterschutzgesetz?“*

All diese Fragen sind für die Begründung eines Beschäftigtenverhältnisses regelmäßig nicht erforderlich. Es spielt auch keine Rolle, dass Bewerberinnen und Bewerber einen Teil dieser Daten typischerweise selbst in ihrer Bewerbung offenlegen (v.a. Geburtsdatum und -ort sowie Lichtbild).

Ergebnis

Das Unternehmen hat sich von Anfang an äußerst einsichtig und kooperativ gezeigt. Sämtliche Bewerberbögen, auch die Bögen bereits eingestellter Mitarbeiterinnen und Mitarbeiter, sind umgehend vernichtet worden.

Nur diesem ungewöhnlichen Maß an Kooperation hat es das Unternehmen zu verdanken, dass ein verhältnismäßig niedriges Bußgeld festgesetzt wurde. Jedoch musste das Unternehmen die Kosten für mein Verwaltungsverfahren tragen.

7.4 Von Technikern, Kostenrechnungen und Krankheiten: Listen des Arbeitgebers

Im Berichtszeitraum habe ich Beratungen und Kontrollverfahren zu unterschiedlichen Listen über Mitarbeiterinnen und Mitarbeiter durchgeführt. Drei dieser Fälle stelle ich hier vor.

Auftraggeber fordert Liste von Technikern zu Identifikation an

Ein Anbieter von Büromaschinen bat um Beratung, da ein Auftraggeber des Unternehmens eine Liste mit Namen, Vornamen und Geburtsdaten der Servicetechnikerinnen und -techniker haben wollte. Mit dieser Liste sollte am Empfang geprüft werden, ob die Technikerin bzw. der Techniker berechtigt sind, dort zu arbeiten. Anrufe vorab oder Mitarbeiterausweise würden nicht ausreichen.

Das bloße Verlangen des Auftraggebers, die Liste herauszugeben, reicht allerdings nicht. Die Weitergabe wäre nicht erforderlich und damit unzulässig nach § 32 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG).

Jedoch könnte der Auftraggeber ein berechtigtes Interesse an der Kenntnis dieser Daten haben. Das kann z.B. der Fall sein, wenn beim Auftraggeber besonders hohe Sicherheitsstandards gelten. Können diese Standards mit Vorab-Anrufen und Mitarbeiterausweisen nicht gehalten werden – beides kann verhältnismäßig leicht vorgetäuscht bzw. gefälscht werden –, kann der Auftraggeber ein berechtigtes Interesse an dieser Liste haben.

Hat der Auftraggeber ein berechtigtes Interesse, wäre die Liste auf das Nötigste zu reduzieren. Zunächst wären nur Technikerinnen und Techniker aufzulisten die für diesen Auftraggeber tatsächlich in Frage kommen. Da der volle Name mit komplettem Geburtsdatum zur Erstellung eines Profils über die Person verwendet werden kann – bis hin zum Identitätsdiebstahl – bietet sich eine Verkürzung der Daten an. So ist „A. Müller, 25.04." – zusammen mit einem Mitarbeiterausweis – eindeutig, ohne dass damit die Sicherheit geschmälert würde.

Speicherung von Namen für die Kosten- und Leistungsrechnung

Bei einem mittelständigen Unternehmen führte ich ein Kontrollverfahren durch. Dort wurde in Teilbereichen eine Projektzeiterfassung für die Kosten-

und Leistungsrechnung (KLR) eingeführt. Die geleisteten Stunden wurden in der Erfassung mit den Namen der jeweiligen Beschäftigten gespeichert, um die konkreten Kosten ermitteln zu können. Dazu bestand im Unternehmen auch eine Betriebsvereinbarung.

Im Kontrollverfahren erläuterte das Unternehmen, dass verschieden qualifizierte Beschäftigte (z.B. Auszubildende, Facharbeiter, Ingenieure) mit unterschiedlicher Gehaltsstruktur an einem Projekt arbeiten. Auch innerhalb der Gruppen gebe es differierende Gehälter.

Einsicht bzw. Auswertungen waren nur den vorgesetzten Bereichsleitungen und dem Personalbereich möglich. Der Zweck wurde durch Betriebsvereinbarung insbesondere auf die KLR beschränkt. Ausdrücklich ausgeschlossen wurde eine Verwendung zur Verhaltens- und Leistungskontrolle.

Bei meiner Bewertung hatte ich auch das Handelsrecht zu berücksichtigen. Unternehmen, die selbst Anlagegüter herstellen, müssen diese auch bewerten. Andernfalls können sie keine richtige Bilanz aufstellen. Es muss daher ein Merkmal geben, mit dem von den geleisteten Stunden auf den gesamten Aufwand geschlossen werden kann. Das war vorliegend der Name, dem ein konkreter Stundensatz zugeordnet werden konnte. Eine alternative Pseudonymisierung war schon nicht möglich, da es keine Gehaltsgruppen gab.

Umfangreiche Liste zu Krankheitsständen

Im folgenden Fall führte ein Klinikum eine zentrale Liste mit den Krankheitsdaten (fast) aller Beschäftigten, weshalb der Betriebsrat um meine Beratung bat. Die Liste war für alle Stationsleitungen des Klinikums zugänglich. Neben den Namen der Beschäftigten waren u.a. die jeweiligen Krankheitszeiten in Stunden bzw. Prozent der Jahres-Arbeitszeit angegeben.

Ich erläuterte, dass lediglich der Personalbereich, die jeweils vorgesetzte Stationsleitung und auch deren Vertretung von aktuellen Krankheitszeiten Kenntnis haben dürfen. Der Personalbereich muss für seine Präventionsarbeit gut zwölf Monate zurückschauen können (z.B. für ein betriebliches Eingliederungsmanagement). Fremde Stationsleitungen benötigen hingegen keinen Zugriff auf diese Informationen.

Von weitergehenden aufsichtsbehördlichen Maßnahmen habe ich bewusst abgesehen. Denkbar wären zwar ein Kontrollverfahren sowie ein Bußgeldverfahren gewesen. Ein solches Eingreifen würde jedoch die vertrauensvolle Zusammenarbeit zwischen Betriebsrat und Arbeitgeber belasten. Sollte der Betriebsrat das Problem mit dem Arbeitgeber nicht selbst einvernehmlich lösen können, kann dieser – oder jede/r Beschäftigte – sich erneut an mich wenden.

Fazit

Dieser Beitrag stellt nur einen kleinen Teilbereich möglicher Listen dar, die Beschäftigte im Arbeitsverhältnis betreffen. Einen berechtigenden Zweck vorausgesetzt, ist die Verarbeitung von Daten in Listen auch möglich. Der Beitrag zeigt zugleich die Grenzen auf. Besonders wenn gesundheitsbezogene – also besonders sensible – Daten betroffen sind. Auch wenn der Empfänger mit Hilfe der Daten Identitätsdiebstahl begehen oder umfangreiche Profile anlegen könnte, ist Vorsicht geboten.

7.5 Kommentierte Gehaltszahlungen: Verwendungszweck bei Kontoauszügen

Der Verwendungszweck bei Lohnüberweisungen ist im Sinne des Beschäftigtendatenschutzes möglichst allgemein zu halten.

Ein Unternehmen überwies seinen Beschäftigten Gehalt und nutzte den „Verwendungszweck" der Überweisung zur näheren Erläuterung des Betrages. Dort fanden sich beispielsweise Bemerkungen wie z.B. „Lohn abzgl. 500,00 Euro nicht erbrachter Auslagen".

Einer der Beschäftigten wandte sich an mich. Er unterhielt bei dem kontoführenden Institut zugleich eine Immobilienfinanzierung. Er befürchtete, das Institut könnte die Erläuterungen des Arbeitgebers im Verwendungszweck nutzen, um seine Kreditwürdigkeit schlechter zu beurteilen.

Bewertung

Für die Durchführung von Beschäftigungsverhältnissen ist die unbare Zahlung von Löhnen und Gehältern erforderlich. Dazu ist die Übermittlung der Bankverbindungen (IBAN, BIC, Name) der Empfänger sowie der Zahlbeträge an die beteiligten Kreditinstitute zwingend.

Gegen eine kurze, sehr allgemein und neutral gehaltene Begründung der Zahlung – z.B. „Gehalt 05/2017" oder „Jahressonderzuwendung" – bestehen keine Bedenken. Der Betrag muss schon deswegen kurz begründet sein, damit der Empfänger die Zahlung zuordnen kann.

Dem Kreditinstitut wurde mit dem ergänzenden Verwendungszweck jedoch eine ergänzende Erläuterung des Zahlbetrages übermittelt. Im konkreten Fall war zudem ein Rückschluss auf vermeintliche Mängel der Arbeitsleistung möglich. Solche Erläuterungen gehen über das hinaus, was bei der Überweisung von Lohn- bzw. Gehaltszahlungen erforderlich ist.

Ergebnis: Sensibilisierung des Arbeitgebers für den Beschäftigtendatenschutz

Erläuterungen der Zahlbeträge haben unmittelbar im Verhältnis zwischen Arbeitgeber und Beschäftigten zu erfolgen. Hierfür bieten sich die regelmäßige Lohn- bzw. Gehaltsabrechnung an. Der Austausch über einen Dritten – z.B. die Bank – ist hingegen nicht erforderlich.

Ich habe das Unternehmen für den Beschäftigtendatenschutz sensibilisiert. Nach meiner Kontaktaufnahme hat es umgehend von solchen Erläuterungen im Zahlungsverkehr mit den eigenen Beschäftigten abgesehen.

7.6 Heimliche Videoüberwachung am Arbeitsplatz: Falsche Auskunft gegenüber der Aufsichtsbehörde

In der Verkaufsstelle eines Unternehmens mit je einer Mitarbeiterin pro Schicht fiel auf, dass die beiden Mitarbeiterinnen unterschiedlich viel Geld einnehmen.
Diese Differenz war offenbar so groß, dass weitere Nachforschungen nötig erschienen. Der Arbeitsplatz wurde mit einer verdeckten Videoüberwachungsanlage (Modell „Rauchmelder“) ausgestattet und überwacht.

Das Unternehmen entschloss sich sogar, der verdächtigten Mitarbeiterin zu kündigen. Die Mitarbeiterin führte anschließend einen Kündigungsschutzprozess bis zum Landesarbeitsgericht Niedersachsen.

Voraussetzungen für die Videoüberwachung

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nach § 32 Abs. 1 Satz 2 BDSG nur erhoben, verarbeitet oder genutzt werden, wenn vorab zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Dies bedeutet, dass es allenfalls ein berechtigtes Interesse an der Überwachung von einzelnen Beschäftigten geben kann, wenn ein begründeter Verdacht besteht, dass konkrete Straftaten begangen wurden und andere Aufklärungsmaßnahmen nicht zur Verfügen stehen bzw. erfolglos geblieben sind (BAG, Urteil vom 21. Juni 2016, Az. 2 AZR 153/11). Dann kann die zeitlich begrenzte Videoüberwachung zulässig sein, wenn das Kontrollinteresse den Persönlichkeitsschutz übersteigt.

Eine heimliche Videoüberwachung ist nur in absoluten Ausnahmefällen zulässig, wenn weniger einschneidende Mittel zur Aufklärung des Verdachts ausgeschöpft sind. Die Videoüberwachung muss damit praktisch die einzig verbleibende Möglichkeit zur Aufklärung darstellen. Sie darf im Hinblick auf den angerichteten Schaden nicht unverhältnismäßig sein.

Die Verhältnismäßigkeit ist insbesondere nicht gewahrt, wenn eine große Zahl von Beschäftigten überwacht würde. Der Arbeitgeber muss daher den Kreis der möglichen Täterinnen und Täter vorab räumlich und funktional abgrenzen.

Der Fall: Überwachung einer Mitarbeiterin

Es war festzustellen, dass weniger einschneidende Mittel nicht ausgeschöpft wurden. Insbesondere gab es vor der Videoüberwachung keine Beobachtung von außen, keine Testkäufe und keine weitergehende Auswertung des Warenwirtschaftssystems. Trotz mehrfacher Aufforderung habe ich im Bußgeldverfahren nicht einmal die Auswertung bekommen, auf die sich die ursprüngliche Kündigung stützte.

Es stellte sich vor den Arbeitsgerichten heraus, dass die Differenz zwischen den beiden Mitarbeiterinnen bei etwa 1% lag. Selbst bei täglichen Umsatzerlösen von 1.000 Euro in der Verkaufsstelle – was angesichts der Branche viel wäre – bedeutet das gerade einmal 5 Euro Abweichung zwischen Vor- und Nachmittagskraft. Bei derart marginalen Abweichungen auf eine Straftat zu schließen, liegt fern.

Vor dem Landesarbeitsgericht hat die Arbeitgeberin dann auch eingeräumt, dass die Videoüberwachung nicht auf fundierter Grundlage erfolgte.

Zusätzlich: Täuschung der Aufsichtsbehörde

Neben den Fragen einer unzulässigen Videoüberwachung ging es in diesem Fall auch um einen weiteren Vorwurf, nämlich den Verdacht einer Falschauskunft des Unternehmens. Im Einzelnen:

Ich wollte vom Unternehmen wissen, welche Tatsachen die Videoüberwachung rechtfertigen sollten. Der Rechtsanwalt des Unternehmens antwortete mir, es habe Kassendifferenzen von etwa 20% bzw. etwa 200 Euro gegeben. Solch eklatante Differenzen hätten tatsächlich einen Verdacht auf eine Straftat begründen können.

Im späteren arbeitsgerichtlichen Verfahren stellte sich allerdings heraus, dass die Differenzen deutlich niedriger waren. Mir gegenüber versuchte das Unternehmen, die 20% bzw. 200 Euro als Kommunikationsfehler zwischen Unternehmen und Rechtsanwalt darzustellen.

Den behaupteten Übermittlungsfehler habe ich nicht gelten lassen. Es widerspricht der Lebenserfahrung, dass diese eine tragende Information nur ein einziges Mal Gegenstand der Mandantengespräche gewesen sein soll und sich der Rechtsanwalt zudem nicht rückversicherte. Ich wurde also bewusst in die Irre geführt.

Konsequenzen

Aufgrund der unzulässigen Videoüberwachung und der Falschauskunft habe ich gegenüber dem Unternehmen zwei Geldbußen im jeweils vierstelligen Bereich festgesetzt. Dass für die unbefugte Videoüberwachung keine höhere Geldbuße ergangen ist, ist vor allem der Kooperation des Unternehmens geschuldet. Ohne diese späte Reue wäre ein höheres Bußgeld in Betracht gekommen.

Festzuhalten bleibt, dass Unternehmen gut beraten sind Ihrer Pflicht zur wahrheitsgemäßen Auskunft nachzukommen. Falsche oder unvollständige Auskünfte sind nach § 43 Abs. 1 Nr. 10 BDSG mit Bußgeldern bis zu 50.000 Euro bedroht.

8. Videoüberwachung

8.1 Videobeobachtung durch öffentliche Stellen: Beratung und Vor-Ort-Termine

Auch in den Jahren 2015 und 2016 wurde meine Beratungstätigkeit zu Fragen der Videoüberwachung durch öffentliche Stellen in Niedersachsen stark nachgefragt. Insgesamt wurde in 118 Fällen mein Rat bzw. meine Unterstützung erbeten, um insbesondere eine Videoüberwachung gemäß § 25a NDSG datenschutzrechtlich einwandfrei zu gestalten.

In mehr als 100 Fällen war es ausreichend, entsprechende Musterdokumente mit Erläuterungen zu übersenden, um die verantwortlichen Stellen in die Lage zu versetzen, Vorabkontrollen, Verfahrensbeschreibungen und Dienstvereinbarungen zu erstellen. Mehrfach wurde ich im Anschluss gebeten, diese Dokumente aus meiner Sicht zu prüfen, auch wenn sie gesetzlich nicht vorlagepflichtig sind. Dieser zusätzlichen arbeitsintensiven Aufgabe bin ich in allen Fällen gerne nachgekommen.

Die restlichen Fälle führten zu einer erweiterten Beratung „vor Ort“, da die jeweiligen Besonderheiten eine Inaugenscheinnahme der zu überwachenden Objekte und Räume voraussetzten. Hierbei handelte es sich insbesondere um Videoüberwachungsanlagen in und an Schulen (vier Vor-Ort-Termine) und Gerichtsgebäuden (sechs Vor-Ort-Termine).

Bei der Videoüberwachung in und an Schulen ist Folgendes zu beachten:

- Während der Schulzeiten ist eine Videoüberwachung grundsätzlich ausgeschlossen, weil sie einen erheblichen Eingriff in die Persönlichkeitsrechte der Schülerinnen, Schüler und Lehrkräfte darstellt, die sich der Überwachung nicht entziehen können, da sie zum Aufsuchen der Schule bzw. zum Aufenthalt in der Schule verpflichtet sind. Außerdem ergibt sich aus § 62 Niedersächsisches Schulgesetz (NSchG) eine Aufsichtspflicht der Schule gegenüber den Schülerinnen und Schülern. Das NSchG enthält keine Erlaubnisnorm, die den Einsatz von Videotechnik erlaubt. Somit können die persönlichen Aufsichtspflichten der Lehrkräfte nicht durch optisch-elektronische Systeme ergänzt oder ersetzt werden.
- Eine Ausnahme kann im Einzelfall die Überwachung der Fahrradständer bzw. des Fahrradkellers und des Parkplatzes sein, da die Nutzung freiwillig ist und der Aufenthalt sich nur auf einen kurzen Zeitraum beschränkt.

Videoüberwachung in Gerichtsgebäuden nur bei Echtzeitkontrolle verhältnismäßig

In und an Gerichtsgebäuden wurden wir mehrfach mit dem datenschutzrechtlichen Problem der sog. Einlasskontrolle per Videoüberwachung konfrontiert. Da die Zweckbestimmung der Videobeobachtung gem. § 25a NDSG dem Schutz von Personen dient, die der überwachten Stelle angehören oder diese besuchen, handelt es sich um eine Rechtsgrundlage, die entstehende bzw. beginnende Gefahren unmittelbar abwehren soll. Daher muss die verantwortliche Stelle in einem sog. „Echtzeitmonitoring" durch berechtigte Personen dafür Sorge tragen, dass bei solchen Gefahrenlagen, die live auf einem Bildschirm zu sehen sind, auch sofort reagiert wird. Beispielsweise kann so unmittelbar verhindert werden, dass eine offensichtlich bewaffnete Person das Gerichtsgebäude betritt, indem die videoüberwachte Eingangstür nicht geöffnet wird. Hingegen ist die Videoüberwachung einer unverschlossenen Eingangstür in Form der Bildaufzeichnung nicht geeignet und damit unverhältnismäßig, um unmittelbar drohende Gefahren wirksam abwehren zu können.

Positive Resonanz auf Beratungen

In allen Beratungsfällen vor Ort habe ich festgestellt, dass meine Hinweise und Ratschläge dankbar angenommen wurden. Es konnte somit sichergestellt werden, dass eine Videoüberwachung nur unter den vom Gesetzgeber festgelegten Voraussetzungen stattfindet. Fragen der Erforderlichkeit und Verhältnismäßigkeit hatten bei den Beratungsterminen ebenso besonderes Gewicht wie Fragen des technisch-organisatorischen Datenschutzes. So ist z. B. bei einer Videoüberwachung mittels Aufzeichnung zwingend zu klären, wer in welchem Umfang und zu welchem Zweck auf das Bildmaterial zugreifen kann. Aufgrund der enormen Nachfrage habe ich jeweils in den Jahren 2015 und 2016 einen Kurs in meinem Datenschutzinstitut zur Videoüberwachung durch die öffentliche Hand angeboten. Beide Kurse waren stark nachgefragt und in kürzester Zeit ausgebucht. Ich werde dieses Kursangebot auch in den kommenden Jahren aufrechterhalten.

8.2 „Videoüberwachung in öffentlichen Verkehrsmitteln“: Datenschutzaufsichtsbehörden veröffentlichen Orientierungshilfe

Das Thema der Videoüberwachung (VÜ) im ÖPNV hatte auch im aktuellen Berichtszeitraum Konjunktur.
So haben sich die deutschen Datenschutzaufsichtsbehörden mit einer im Herbst 2015 herausgegebenen Orientierungshilfe „Videoüberwachung in öffentlichen Verkehrsmitteln“ ausführlich zu der Frage geäußert, unter welchen Voraussetzungen VÜ im ÖPNV datenschutzrechtlich zulässig ist[1]. Auch diese Orientierungshilfe kommt zu dem Ergebnis, dass eine uneingeschränkte VÜ der Fahrgastbereiche nicht in Betracht kommt.

Die Orientierungshilfe ist vom Düsseldorfer Kreis, dem Koordinierungs- und Abstimmungsgremium aller deutschen Datenschutzaufsichtsbehörden, als Beschluss gebilligt worden.

…und mittlerweile mit (verkehrs-)politischer Dimension

Allerdings wird über die Grenzen der Bundesländer hinweg seit einiger Zeit das verkehrspolitische Ziel verfolgt, alle Fahrzeuge des Personennahverkehrs mit umfassender Videotechnik auszustatten.

Es wird in dem Zusammenhang verlangt, eine „flächendeckende, tageszeitunabhängige Videoaufzeichnung in öffentlichen Verkehrsmitteln (…)“ zu schaffen[2]. Die Verkehrsministerkonferenz (VMK) verleiht in ihrem Beschluss ihrer Sorge Ausdruck, dass die Orientierungshilfe „einer weiteren Entwicklung dieses Sicherheitskonzeptes entgegensteht.“ Die VMK bittet daher in demselben Beschluss die Innenministerkonferenz, „im Sinne einer einheitlichen Sicherheitsphilosophie im öffentlichen Personenverkehr darauf hinzuwirken, die geltenden datenschutzrechtlichen Vorgaben entsprechend den Regelungen im Bundespolizeigesetz anzupassen“.

Dieser Appell der VMK hat seine Wirkung in der Politik offenbar nicht verfehlt.

1 Beschluss des Düsseldorfer Kreises vom 16.09.2015 https://www.lfd.niedersachsen.de/download/101172

2 Beschluss der VMK am 14./15.04.2016 in Heringsdorf; Geschäftsstelle der VMK K 1 – 1 Bd. 124

Jedenfalls haben sich zahlreiche Innenminister und -politiker nach den terroristischen Anschlägen und Amokläufen im Sommer 2016 in Nizza, München, Würzburg und Ansbach angesichts des in der Bevölkerung wachsenden Gefühls von Unsicherheit für eine Ausweitung der Kameraüberwachung im öffentlichen Raum und auch im ÖPNV eingesetzt.
Dies hat im Herbst 2016 zu der gesetzgeberischen Initiative des Bundesinnenministeriums geführt, die Videovorschrift im Bundesdatenschutzgesetz (BDSG) mit dem Ziel zu ergänzen, damit einen Beitrag zur Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im ÖPNV zu leisten (Videoüberwachungsverbesserungsgesetz)[3].

Vor dem Hintergrund der Positionierung der Datenschutzaufsichtsbehörden in ihrer Orientierungshilfe ist es allerdings nicht verwunderlich, dass die 92. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder im November 2016 zu der legislativen Initiative des Bundesinnenministers zur Ergänzung des § 6b BDSG eine klar ablehnende Position bezogen hat[4]. Sie hat nicht nur darauf hingewiesen, dass der Gesetzentwurf nicht zu begründen vermag, dass die angestrebte Erleichterung der VÜ die öffentliche Sicherheit besser gewährleisten kann, als das gegenwärtig der Fall ist. Sie hat vielmehr auch deutlich gemacht, dass der Ansatz des Bundesinnenministers, nicht-öffentliche Stellen, also private Betreiber insbesondere von Einkaufszentren und des ÖPNV mit der VÜ zum Schutz von Leben, Gesundheit oder Freiheit von Personen zu betrauen, hoch problematisch ist. Dadurch wird jedenfalls dem Prinzip unseres Rechtsstaates, die Wahrnehmung der Gefahrenabwehr ausschließlich den staatlichen Sicherheitsbehörden als Aufgabe zuzuweisen, in keiner Weise Rechnung getragen.

Videoüberwachung kann bereits heute einen Beitrag zu einem durchdachten Sicherheitskonzept leisten

Abseits dieser hoch emotionalen Diskussion über die Frage, welchen Sicherheitsbeitrag Videoüberwachungstechnik im öffentlichen Raum überhaupt leisten kann, bleibt allerdings festzustellen, dass ein datenschutzkonformer Einsatz von Kameras im ÖPNV bereits jetzt möglich ist. Die sowohl im Beschluss der Verkehrsministerkonferenz als auch im Entwurf eines Videoüberwachungsverbesserungsgesetzes (s.o.) zum Ausdruck kommende Sorge, dass der Datenschutz ein angemessenes Sicherheitskonzept behindern könnte, ist jedenfalls unbegründet.

Allerdings muss jedes Sicherheitskonzept zur Zielerreichung geeignet sein und sich um Ausgewogenheit und insbesondere um Verhältnismäßigkeit bemühen. Dafür muss aber das Recht nicht geändert werden.

Eine datenschutzrechtliche Bewertung der VÜ hat zunächst bei der Frage nach der einschlägigen Rechtsgrundlage anzusetzen. Welches Gesetz anzuwenden ist, richtet sich danach, ob das Verkehrsunternehmen privatrechtlich organisiert ist oder ob es sich um eine öffentlich-rechtlich organisierte Einrichtung handelt.

3 Das Gesetz wurde am 28.04.2017 verkündet. http://dipbt.bundestag.de/extrakt/ba/WP18/788/78834.html

4 Entschließung der 92. DSK vom 09.11.2016: „Videoüberwachungsverbesserungsgesetz" zurückziehen! http://www.lfd.niedersachsen.de/download/112520

So ist auf privatrechtlich organisierte Unternehmen das BDSG anzuwenden, während für öffentliche Stellen des Landes das Niedersächsische Datenschutzgesetz gilt. Inhaltlich unterscheiden sich die Gesetze weniger in den Anforderungen, die an eine rechtmäßige VÜ gestellt werden, sondern vor allem im Hinblick auf die Sanktionierungsmöglichkeiten bei Rechtsverstößen.
Dieser Umstand spielt eine große Rolle bei der rechtlichen Auseinandersetzung um eine datenschutzaufsichtliche Anordnung, die ich auf der Grundlage des BDSG gegenüber einem Nahverkehrsunternehmen mit dem Ziel, die in den Fahrzeugen dieses Unternehmens betriebene zeitlich und räumlich umfassend betriebene VÜ einzustellen, ausgesprochen hatte. Die von dem Verkehrsunternehmen gegen meine Anordnung erhobene verwaltungsgerichtliche Klage hat im Berichtszeitraum allerdings nicht zu einer Klärung der Frage geführt, ob die von dem Unternehmen betriebene umfängliche VÜ datenschutzkonform erfolgt. Vor dem zuständigen Verwaltungsgericht Hannover ging es vielmehr ausschließlich um die Frage nach dem anzuwendenden Recht: Ist das klagende Nahverkehrsunternehmen, eine AG und damit juristische Person des Privatrechts, ein privates Unternehmen – so meine Auffassung – oder als ein nicht am Wettbewerb teilnehmendes und von dem öffentlichen Aufgabenträger beherrschtes Unternehmen anzusehen?

Das Verwaltungsgericht ist in seinem Urteil vom Februar 2016 überraschenderweise zu der Auffassung gelangt, das Verkehrsunternehmen sei einer öffentlichen Stelle gleichzusetzen, weshalb der Rechtsstreit nach Niedersächsischem Datenschutzrecht zu beurteilen und eine Anordnung, wie ich sie gegenüber dem Unternehmen ausgesprochen habe, nicht statthaft sei[5]. Zu der eigentlich interessierenden datenschutzrechtlichen Frage zur Zulässigkeit einer umfassenden VÜ im ÖPNV hat sich das Gericht leider nicht geäußert. Deshalb habe ich gegen dieses Urteil Berufung eingelegt[6].

Die gegenwärtige Rechtslage

Trotz der Entscheidung des Verwaltungsgerichts Hannover gehe ich daher gegenwärtig davon aus, dass die VÜ im ÖPNV, soweit sie von privatrechtlich organisierten Verkehrsunternehmen betrieben wird, nach der speziellen Rechtsvorschrift des § 6b BDSG zu beurteilen ist. Diese Vorschrift ist im Jahr 2001 in das Gesetz eingefügt worden. Betrachtet man einmal die Parlamentsdebatten zu dieser gesetzlichen Neuerung aus dem Jahr 2001, so wurde schon damals ausdrücklich von einem „Wildwuchs" im Bereich der VÜ gesprochen. Die gesetzliche Regelung, so hieß es im Bundestag, ziele deshalb darauf ab, „jede unnötige und überflüssige" Überwachung zu verhindern. Dem Gesetzgeber ging es also dezidiert um eine Einschränkung und Rückführung der schon damals verbreiteten VÜ auf ein angemessenes Maß (BT-Drs. 14/5793). Auch in der amtlichen Gesetzesbegründung heißt es ausdrücklich, dass mit der Norm das Ziel verfolgt werden soll, „insgesamt eine restriktivere Verwendungspraxis herbeizuführen".
Die den Datenschutzaufsichtsbehörden in der aktuellen öffentlichen Diskussion über die Frage der Notwendigkeit der Ausweitung von VÜ im öffentlichen Raum vorgehaltene zu restriktive Aufsichtspraxis ist vor diesem Hintergrund ungerechtfertigt.

5 Urteil des VG Hannover vom 10.02.2016 – 10 A 4379/15 -

6 Pressemitteilung vom 04.04.2016: https://www.lfd.niedersachsen.de/startseite/allgemein/presseinformationen/datenschutzbeauftragte_legt_berufung_gegen_urteil_verwaltungsgerichts_hannover_zur_uestravideoueberwachung_ein/datenschutzbeauftragte-fordern-nachbesserung-in-wesentlichen-punkten-142208.html

Der datenschutzrechtliche Maßstab für die VÜ im ÖPNV ist und bleibt also § 6b BDSG, der mehr oder weniger normenklar definiert, unter welchen Voraussetzungen Videotechnik überhaupt installiert und betrieben werden darf.

Nach § 6b BDSG kann Videotechnik durch nicht-öffentliche Stellen eingesetzt werden, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Ein zulässiger Zweck ist also die VÜ zur Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG). Das Hausrecht umfasst zunächst die Befugnis, darüber zu entscheiden, wem der Zutritt zu einem bestimmten Ort gestattet wird. Bei Verkehrsunternehmen, die der Beförderungspflicht unterliegen, spielt diese Befugnis naturgemäß keine große Rolle.
Vom Hausrecht ist allerdings auch die Befugnis umfasst, das Zutrittsrecht und das Recht zum Verbleib von der Erfüllung bestimmter Bedingungen abhängig zu machen – etwa von der Bezahlung eines Beförderungsentgelts oder von der Nichtkonsumierung von Alkohol.
Deshalb ist das Hausrecht fraglos auch ein Thema für die Verkehrsunternehmen, so dass zur Wahrnehmung des Hausrechts grundsätzlich auch VÜ in Betracht kommt. Allerdings kommt nur der Videotechnikeinsatz in Betracht, der zur Zweckerreichung auch geeignet ist.

Bei der VÜ wird zwischen dem Monitorverfahren und dem Black-Box-Verfahren unterschieden.

Beim Monitorverfahren wirkt die Kamera gewissermaßen als „verlängertes Auge". Die von der Kamera aufgezeichneten Aufnahmen werden in Echtzeit in eine Leitstelle übertragen und dort „live" angesehen. Diese Echtzeitüberwachung ermöglicht im Ernstfall eine sofortige Intervention. Beim Black-Box-Verfahren findet hingegen keine Echtzeitüberwachung statt. Bei diesem Verfahren zeichnen die Kameras lediglich auf, und nach einem bestimmten Zeitraum werden die Aufzeichnungen wieder überschrieben. Entscheidend ist nun, dass die Wahrnehmung des Hausrechts eine sofortige Intervention voraussetzt. Reine Black-Box-Systeme, die lediglich aufzeichnen, ohne dass eine Echtzeitüberwachung stattfindet, sind nach alledem für die Wahrnehmung des Hausrechts von vornherein nicht geeignet. Die VÜ in öffentlichen Verkehrsmitteln erfolgt in der Praxis allerdings nahezu ausschließlich nach dem Black-Box-Verfahren, so dass die Wahrnehmung des Hausrechts hier nicht als zulässiger Zweck betrachtet werden kann.

Zulässig ist die VÜ allerdings auch dann, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erfolgt (§ 6b Abs. 1 Nr. 3 BDSG).

Die VÜ im ÖPNV soll im Regelfall potenzielle Täter von der Begehung von Straftaten gegen Personen oder Sachen in den Verkehrsmitteln abhalten, bei der Aufklärung begangener (Straf-)Taten helfen und das Sicherheitsgefühl der Fahrgäste erhöhen.
Dies sind jedenfalls die klassischen Zwecke, mit denen regelmäßig nicht nur Verkehrsunternehmen, sondern auch Verkehrs- und neuerdings auch Innenminister das Erfordernis eines umfassenden Kameraeinsatzes begründen.
Es ist allerdings fraglich, ob mit diesen drei Zwecken berechtigte Interessen im Sinne des BDSG verfolgt werden. Zwar soll nicht in Abrede gestellt werden, dass die Verkehrsunternehmen von dem Wunsch geprägt sind, zur – vermeintlichen – Gewährleistung eines hohen Maßes an subjektivem Sicherheitsgefühl der Fahrgäste eine möglichst umfassende VÜ im Black-Box-Verfahren betreiben zu wollen.

Das subjektive Sicherheitsempfinden der Bevölkerung ist zweifellos ein ernstzunehmender politischer Faktor. Die datenschutzrechtlich entscheidende Frage ist jedoch, ob eine VÜ nach dem Black-Box-Verfahren – also ein Kameraeinsatz ohne jegliche sofortige Interventionsmöglichkeit – tatsächlich mit dem Wunsch gerechtfertigt werden kann, eine Steigerung des Sicherheitsgefühls der Fahrgäste bewirken zu wollen. „Was ein berechtigtes Interesse sein kann, … muss objektiv begründbar sein", so die Gesetzesbegründung zu § 6b BDSG (BT-Drs. 14/5793). Hier zählen also Fakten, nicht Gefühle. Aus zahlreichen kriminologischen Untersuchungen wissen wir zudem, dass sich das Sicherheitsgefühl der Bürgerinnen und Bürger vom tatsächlichen Bedrohungspotenzial oft ganz erheblich unterscheidet. Auch deshalb kann allein die Berufung auf ein Sicherheitsgefühl noch kein berechtigtes Interesse am Einsatz von Videotechnik begründen. Demgegenüber kommen der Abschreckungseffekt und das Ziel, begangene (Straf-)Taten aufzuklären, die Kameras also zur Beweissicherung einzusetzen, zwar grundsätzlich als berechtigte Interessen in Betracht. Die Landesregierung war allerdings im Berichtszeitraum trotz zweier parlamentarischer Anfragen (LT-Drs. 17/5487 und 17/5613) nicht zu einer Auskunft in der Lage, in wie vielen Fällen Videomaterial aus der ÖPNV-Überwachung tatsächlich zur Ermittlung eines Beschuldigten und damit zur Einleitung eines strafrechtlichen Ermittlungsverfahrens geführt hat. Insoweit ist eine sicherheitserhöhende Wirkung der Kameraüberwachung in Bussen und Bahnen jedenfalls für Niedersachsen nicht empirisch belegt. Dies deckt sich mit der Feststellung des Direktors des Kriminologischen Forschungsinstituts Niedersachsen in einem Zeitungsinterview, wonach sich Straftäter von mehr VÜ nicht abschrecken lassen. Im Übrigen ist auch die im Rahmen der bekannten Fahrgastbefragungen immer wieder geäußerte Furcht vor Übergriffen durch objektive Zahlen nicht belegbar. Es gibt ausweislich der aktuellen polizeilichen Kriminalstatistiken keinerlei Anlass, etwas anderes zu vermuten. Auch die Verkehrsunternehmen konnten mir gegenüber bisher nicht schlüssig darlegen, dass Fahrgäste in erhöhtem Maße der Gefahr ausgesetzt sind, Opfer von Straftaten in den Fahrzeugen des ÖPNV zu werden. Eine umfassende VÜ kann also im ÖPNV weder mit einem höheren Abschreckungseffekt noch mit einer verbesserten Strafverfolgung begründet werden. Die Befürchtungen der Fahrgäste, im ÖPNV bei reduzierter VÜ einem hohen Straftatenrisiko ausgesetzt zu sein, sind zudem objektiv nicht belegbar.
Als relevanter Aspekt eines berechtigten Interesses im Sinne des § 6b BDSG bleibt somit nur der Umstand, dass die Träger des öffentlichen Personennahverkehrs, also das Land und die Kommunen, in ihren Streckenausschreibungen regelmäßig den umfassenden Einsatz von VÜ verlangen. Diese vertraglich von den Verkehrsunternehmen übernommene Pflicht zum Kameraeinsatz entbindet sie aber nicht von ihrer Pflicht, die VÜ in der Praxis datenschutzkonform auszugestalten. Letztlich entscheidend ist deshalb die Frage, ob der Kameraeinsatz im konkreten Einzelfall erforderlich ist, und ob Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen.

Das Gesetz verlangt damit eine umfassende einzelfallbezogene Verhältnismäßigkeitsprüfung, in deren Mittelpunkt eine Abwägung zwischen den Interessen der Verkehrsunternehmen auf der einen und den Interessen der überwachten Fahrgäste auf der anderen Seite steht.

Die VÜ stellt unstreitig einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz), das auch europarechtlich in Art. 8 der EU-Grundrechte-Charta verbürgt ist. Das Datenschutzgrundrecht umfasst im Kern das Recht jedes Menschen, sich in der Öffentlichkeit frei und unbeobachtet zu bewegen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer VÜ zu werden. Dabei ist dieses Grundrecht unteil-

bar und unterliegt auch keiner graduellen Differenzierung nach Schwere oder Intensität einer Persönlichkeitsrechtsverletzung.
Insofern ist es auch unerheblich, welche Eingriffsintensität die in den Fahrzeugen der Verkehrsunternehmen betriebene VÜ hat und ob das ausschließlich verwendete Black-Box-Verfahren die Beeinträchtigung mildert. Entscheidend ist vielmehr, dass die Unternehmen durch die (Video-)Datenerhebung und -verarbeitung in jedem Fall einen Eingriff in das informationelle Selbstbestimmungsrecht der davon betroffenen Fahrgäste vornehmen. Auf der anderen Seite steht das Interesse der Verkehrsunternehmen, sich gegenüber den Trägern des öffentlichen Personennahverkehrs möglichst vertragstreu zu verhalten. Auch diese Interessen können Verfassungsrang haben.

Wer VÜ dazu nutzen will, um Straftaten aufzuklären oder gar präventiv zu verhindern, der muss zunächst nachweisen, dass tatsächlich ein bestimmtes Straftatenrisiko besteht. Es muss also eine hinreichende Wahrscheinlichkeit dafür bestehen, dass auf den befahrenen Strecken tatsächlich Körperverletzungen, Vermögensdelikte, Sachbeschädigungen oder sonstige Rechtsverletzungen begangen werden. Eine nur abstrakte Gefahrenlage rechtfertigt jedenfalls den tiefen Grundrechtseingriff, der mit dem zeitlich und räumlich umfassenden Kameraeinsatz in den Fahrzeugen des ÖPNV und des SPNV verbunden ist, nicht.

Die Datenschutzaufsichtsbehörden verlangen deshalb, dass es auf den konkreten Strecken, auf denen die Verkehrsunternehmen Videotechnik einsetzen wollen, in der Vergangenheit bereits nachweislich zu Straftaten gekommen ist. Erforderlich ist damit eine seriöse Gefahrenprognose. Die Verkehrsunternehmen müssen dokumentieren, dass die VÜ in ihrem konkret praktizierten Umfang tatsächlich zur Abwehr ganz konkreter Gefahren erforderlich ist. Ein Einsatz der Videotechnik „bloß auf Verdacht" ist deshalb rechtswidrig. Und allein wegen eines einmaligen Vorfalls in der Vergangenheit besteht nicht notwendigerweise eine Wiederholungsgefahr für die Zukunft. Die vom BDSG vorgeschriebene Interessenabwägung führt letztlich in der Praxis dazu, dass eine permanente und undifferenzierte VÜ im öffentlichen Personennahverkehr in aller Regel zu einem unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung führt. Nicht zuletzt auch das Gebot der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) verlangt regelmäßig eine zeitliche und räumliche Beschränkung der VÜ.

Im ÖPNV kommt daher in aller Regel nur eine zeitweilige VÜ in Betracht, die zudem nur Teilbereiche des Raumes erfassen darf. Der konkreten Gefahrenprognose entsprechend kann etwa auch ein Kameraeinsatz nur zu bestimmten Tages- oder Nachtzeiten zulässig sein. VÜ im ÖPNV kann daher datenschutzkonform betrieben werden. Ein die derzeitige Sicherheitsdebatte prägender Einsatz der Videotechnik nach der Gießkannenmethode unter dem Motto „viel hilft viel" entspricht allerdings nicht den Anforderungen des BDSG.

8.3 Heimliche Überwachung mit Spionagekameras

Ob in Kugelschreibern, Powerbanks, Lautsprecherboxen oder auch in Kinderspielzeug, immer häufiger finden sich in diesen Alltagsgegenständen versteckte Spionagekameras, die zudem oft auch über eine Audiofunktion verfügen. Heute sind solche Produkte längst in Serie gegangen, zu Preisen, die für jedermann erschwinglich sind.

Da sie als Kameras nicht erkannt werden, ist mit diesen verkleideten Kameras eine heimliche Videofernüberwachung oder auch das heimliche Abhören möglich. Das gefährdet die Persönlichkeitsrechte der davon Betroffenen.

Der Betrieb einer solchen Kamera ist daher unzulässig. Nach § 90 Telekommunikationsgesetz (TKG) ist es verboten, Sendeanlagen oder sonstige Telekommunikationsanlagen zu besitzen, herzustellen, zu vertreiben, einzuführen oder sonst in den Geltungsbereich dieses Gesetzes zu verbringen, die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind und auf Grund dieser Umstände oder auf Grund ihrer Funktionsweise in besonderer Weise geeignet und dazu bestimmt sind, das nicht öffentlich gesprochene Wort eines anderen von diesem unbemerkt abzuhören oder das Bild eines anderen von diesem unbemerkt aufzunehmen.

Maßgeblich ist, dass es sich um eine drahtlose Kommunikation handelt, was aber in der heutigen WLAN-Welt bei diesen Dingen überwiegend der Fall sein dürfte.

Die Folgen sind nicht unerheblich, denn wer eine solche Sendeanlage oder eine sonstige Telekommunikationsanlage besitzt oder herstellt, vertreibt, einführt oder sonst in den Geltungsbereich dieses Gesetzes verbringt, wird gem. § 148 Abs. 1 Nr. 2 TKG mit Freiheitsstrafe bis zu zwei Jahren oder mit einer Geldstrafe bestraft.

Sollte ich im Rahmen einer Eingabe oder einer Datenschutzkontrolle auf solche Kameras stoßen, werde ich den Fall ohne weitere Prüfung an die zuständige Bundesnetzagentur abgeben, die die Vernichtung dieser Gegenstände anordnen und den Nachweis der Vernichtung verlangen kann (§ 115 Abs. 1 TKG).

8.4 Datenschutzgerechtes Sicherheitskonzept für Taxis umgesetzt

Immer wieder wurde aufgrund diverser Überfälle auf Taxifahrer der Wunsch an mich herangetragen, dem Einsatz von Videokameras zum Schutz der Fahrer zuzustimmen.

Die Datenschutzaufsichtsbehörden haben dazu eine gemeinsame und einvernehmliche datenschutzrechtliche Beurteilung vorgenommen und bereits im Februar 2013 einen Beschluss gefasst, wonach eine Videoüberwachung im Taxi unter engen Voraussetzungen in Betracht kommt.[1]
Bereits in meinem XXI. Tätigkeitsbericht hatte ich daher darauf hingewiesen, dass sich auch die Zulässigkeit einer Videoüberwachung durch Taxi-Unternehmen nach § 6b BDSG bestimmt und das betroffene Taxi-Unternehmen als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen in Betracht ziehen muss, bevor eine uneingeschränkte Videoüberwachung des Fahrgastraumes erwogen werden kann.

Nach intensiven Beratungsgesprächen mit Mitarbeitern meines Hauses hat nun ein Taxi-Unternehmen aus Hannover ein den Vorgaben des o.g. Beschlusses entsprechendes Konzept zum datenschutzgerechten Einsatz von Kameras in den Fahrgasträumen der Taxis erarbeitet und umgesetzt, das die folgende Struktur aufweist :

Nach dem Einstieg eines Fahrgastes und der Aktivierung des Taxameters werden innerhalb von zwei Minuten zwölf Einzelbilder des Fahrgastinnenraums gefertigt und nach 24 Stunden wieder automatisch gelöscht. Dem Beschäftigtendatenschutz wird dadurch Rechnung getragen, dass dabei der Fahrerbereich nicht erfasst wird.
Diese Bilder werden verschlüsselt abgelegt und sind so vor dem unbefugten Zugriff geschützt. Nur im Falle einer Alarmauslösung nach einem etwaigen Übergriff des Fahrgastes wird durch die Fahrerin oder den Fahrer des Taxis zugleich eine permanente Videoaufzeichnung gestartet. In diese erhalten die Mitarbeiter der Taxizentrale, die über diesen Notruf benachrichtigt wird, zugleich Einblick in die Videoaufnahmen in Echtzeit und können weitere Maßnahmen zum Schutz des Taxifahrers ergreifen.

Bei der Prüfung der Erforderlichkeit dieses Kamera-Einsatzkonzeptes hat das Taxiunternehmen auch berücksichtigt, dass bspw. bei wiederkehrenden Krankentransporten, bei denen die Fahrgäste bekannt sind. Deshalb wird dann auf die Anfertigung von Aufnahmen verzichtet.

Dieses Konzept wird von mir insbesondere deshalb begrüßt, weil es die Eingriffsintensität in die Grundrechte des Fahrgastes und der Fahrerin bzw. des Fahrers auf das absolut notwendige Minimum reduziert und zugleich den berechtigten Schutzanliegen der Taxifahrer angemessen Rechnung trägt.

1 Beschluss des Düsseldorfer Kreises „Videoüberwachung in und an Taxis“: https://www.lfd.niedersachsen.de/download/85569

8.5 Unzulässige Videoüberwachung am Hafenbecken

Mir wurde eine Eingabe vorgelegt, wonach der Hafenbereich einer Ostfriesischen Insel weiträumig überwacht wurde, einschließlich der Zugänge zu den öffentlichen Toiletten und zu einem anliegenden Restaurant.

Diese Kameras wurden von einer Reederei betrieben, die in der Vergangenheit immer wieder mit den Folgen von Vandalismus kämpfen musste, wenn Gegenstände in das Hafenbecken geworfen wurden und so der Inselversorgungsverkehr gefährdet wurde. Zudem gab es einen Einbruchsversuch an dem Restaurant.

Bei dem Hafengelände handelt es sich um öffentlich zugänglichen Raum, sodass die Zulässigkeit der Videoüberwachung nach Maßgabe des § 6b Abs. 1 Nr. 2 und 3 und Abs. 3 BDSG zu prüfen war. Eine Videoüberwachung muss demnach zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke geeignet und erforderlich sein und es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Berechtigtes Interesse und geeignete Rechtsgrundlage für Videoüberwachung nicht vorhanden

Ein als Anlass benannter Einbruchsversuch erfolgte nicht bei der Reederei, weshalb insoweit ein eigenes berechtigtes Interesse an der Videoüberwachung nicht erkennbar war. Die Zulässigkeit der Überwachung war daher zu verneinen. Hinzu kam, dass auch die Videoüberwachung der Zugänge zu den Toilettenräumen schon deshalb zu beanstanden war, weil die Überwachung solcher Bereiche, die nicht mehr zur sogenannten Sozialsphäre gehören und besonderem Schutz unterliegen, in jedem Fall unzulässig ist.

Eine zwischen der Reederei und ihrem Betriebsrat geplante Betriebsvereinbarung konnte nicht als Rechtsgrundlage für die Überwachung öffentlich zugänglicher Bereiche herangezogen werden. Eine Betriebsvereinbarung kann nur die Rechtbeziehungen innerhalb des Beschäftigungsverhältnisses regeln und ist daher nicht als Rechtsgrundlage für die Überwachung öffentlicher Bereiche, die im Wesentlichen von betriebsfremden Personen frequentiert werden, nutzbar.

Aufgrund des Fehlens einer Erlaubnisnorm waren die fünf Kameras im Hafenbereich daher umgehend außer Funktion zu nehmen.

Neben den Kameras, die Anlass für die Prüfung waren, überwachte die Reederei mit 64 weiteren Kameras die Terminals (Innen- und Außenbereiche) an anderen Standorten. Darüber hinaus wurden die eingesetzten Schiffe mit diversen Kameras überwacht.

Die Zwecke der Videoüberwachung waren dabei vielfältig. Neben der Beweissicherung im Falle von Straftaten (Vandalismus, Einbruch, Diebstahl) wurde die Überwachung zur Verbesserung des Betriebsablaufes durchgeführt. Auf den Schiffen diente die dort im reinen Monitoring-Modus durchgeführte Videoüberwachung der Unterstützung beim Manövrieren des Schiffes (An- und Ablegemanöver) und der Kontrolle der manuell zu öffnenden Evakuierungspforten. Die zu diesen berechtigten Zwecken eingesetzten Kameras haben die Interessen der davon u.U. betroffenen Personen nicht relevant tangiert und wurden daher von mir nicht beanstandet.

Die Schutzbedürftigkeit der Interessen der von der Videoüberwachung betroffenen Personen in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, ist allerdings generell als besonders hoch einzustufen. Dies trifft auf die für Gäste eingerichteten Sitzbereiche, durch die ein längerer Aufenthalt ermöglicht wird, im besonderen Maße zu. Daher werden die Persönlichkeitsrechte der sich dort länger aufhaltenden Gäste durch eine ständige Videoüberwachung erheblich beeinträchtigt. Diese Bereiche in den Terminals, auf den Schiffen und auch auf dem Hafengelände mussten daher während der Öffnungszeiten durch Verpixeln oder Schwenken der Kamera aus der Überwachung ausgenommen werden.

Videoüberwachung während der Betriebszeit meist unzulässig

Beschäftigte haben einen Anspruch darauf, bei Ausübung ihrer beruflichen Tätigkeit keiner ständigen Arbeits- und Leistungskontrolle seitens des Arbeitgebers zu unterliegen.
Lediglich der begründete Verdacht auf eine konkrete Straftat kann nach § 32 Abs. 1 S. 2 BDSG ein berechtigtes Interesse an der Überwachung einzelner Beschäftigter darstellen. Die Überwachungen einer Baustelle, des Personaleingangs und der Tresen können eine unzulässige Mitarbeiterüberwachung ermöglichen und sind daher i.d.R. während der Betriebszeiten ebenfalls unzulässig.

Für die Steuerung der Arbeitsabläufe ist eine Aufzeichnung nicht erforderlich. Für operative Zwecke ist Videoüberwachung überhaupt nur mit angeschlossenem Monitoring und Interventionsmöglichkeiten geeignet. Die Aufzeichnung für die zu operativen Zwecken eingesetzten Kameras musste folglich unterbleiben.

Die Speicherdauer von 30 Tagen der Aufzeichnungen der Kassenkameras, die auch zur Aufklärung von Kassendiskrepanzen herangezogen wurden, entspricht nicht den datenschutzrechtlichen Anforderungen des § 6b Abs. 5 BDSG, wonach die Daten unverzüglich zu löschen sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen entgegenstehen. In der Gesetzesbegründung heißt es hierzu, dass die Prüfung angefallenen Videomaterials zur Bedarfsklärung unverzüglich, d. h. in der Regel innerhalb von ein bis zwei Arbeitstagen, vorzunehmen ist. Unter Berücksichtigung eventuell arbeitsfreier Zeiten an den Wochenenden sind die Daten nach spätestens 72 Stunden zu löschen. Einer Speicherdauer, die regelmäßig 72 Stunden überschreitet, stehen sowohl das Gebot der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) als auch die schutzwürdigen Interessen der Betroffenen entgegen.

Reederei folgt Empfehlungen und behebt festgestellte Mängel

Alle Hinweise zur Ausgestaltung der Videoüberwachung wurden von der Reederei umgehend bearbeitet und umgesetzt. Neben der Begrenzung der Speicherfrist auf 72 Stunden bei den Kameras, bei denen eine Speicherung gem. § 6b Abs. 3 BDSG zulässig ist, wurden bei zwei Kameras die Zeiten, zu denen die Kameras aktiviert sind, begrenzt. Sechs Kameras wurden außer Funktion genommen und bei weiteren acht Kameras Verpixelungen der kritischen Bereiche vorgenommen.

Als ein besonderes Problem stellte sich im Rahmen meiner Prüfung heraus, dass das Unternehmen zwar einen Datenschutzbeauftragten bestellt hatte, dieser aber offensichtlich nicht über die erforderliche Fachkunde i.S.d.§ 4f Abs.2 BDSG verfügte.
Neben der teilweise beanstandeten Ausgestaltung der Videoüberwachung lagen weder eine Vorabkontrolle noch ein Verfahrensverzeichnis vor. Die Beschäftigten, die auf die Bilddaten berechtigten Zugriff haben, sind zudem nicht auf das Datengeheimnis gem. § 5 BDSG verpflichtet worden. An den Hinweisschildern zur Videoüberwachung fehlte die Nennung der verantwortlichen Stelle, die gem. § 6b Abs. 2BDSG neben dem Umstand der Beobachtung erkennbar zu machen ist.

Aufgrund der fehlenden Fachkunde lag keine wirksame Bestellung einer/eines Datenschutzbeauftragten nach § 4f BDSG vor. Im vorliegenden Fall ergab sich eine Bestellpflicht aber bereits aus der Erforderlichkeit einer Vorabkontrolle (§ 4d Abs. 5 BDSG), die der betriebliche Datenschutzbeauftragte durchführen muss.

Auch hier hat das Unternehmen sofort reagiert. Die Qualifizierung des Datenschutzbeauftragten wurde umgehend nachgeholt und anschließend alle erforderlichen Maßnahmen umgesetzt.

8.6 Videokameras überwachen Tankräuber und Tankstellenmitarbeiter

Dass Tankstellen mit Videoüberwachungskameras ausgestattet sind ist nahezu eine Selbstverständlichkeit.
Schließlich ist allerorten von Tankdiebstählen und Überfällen zu lesen.
Die Überwachung der Tanksäulen zur Aufdeckung und Sicherung von Beweisen bei Tankdiebstählen ist daher auch grundsätzlich nicht zu beanstanden. Trotzdem muss man im Detail auf Folgendes achten:

Die Speicherdauer

Nach § 6b Abs. 5 BDSG sind die Videobilder unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.
In der Gesetzesbegründung heißt es hierzu, das die verantwortliche Stelle verpflichtet ist, die Prüfung angefallenen Videomaterials zur Bedarfsklärung unverzüglich, d. h. in der Regel innerhalb von ein bis zwei Arbeitstagen, vorzunehmen.

Unter der Annahme, dass Tankstellen zudem meist täglich geöffnet haben, oft sogar rund um die Uhr, ist daher eine Speicherdauer von 48 Stunden ausreichend. In begründeten Fällen kann diese auf max. 72 Stunden beschränkt werden, danach sind die Videobilder zu löschen, am wirksamsten durch eine automatisierte periodische Löschung, etwa durch Selbstüberschreiben.

Das Hinweisschild

Bei einer zulässigen Videoüberwachung sind gem. § 6b Abs. 2 BDSG der Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen erkennbar zu machen. Zudem ist der Hinweis so anzubringen, dass der Kunde diesen beim Eintritt bzw. bei Tankstellen beim Einfahren in den überwachten Bereich direkt im Blick hat.
Eine Möglichkeit wäre z.B. die Anbringung des Hinweisschildes an der Stele bei der Einfahrt. Darüber hinaus wäre es auch denkbar, an den tragenden Säulen mit Blickrichtung der einfahrenden Kfz, entsprechend große Hinweisschilder anzubringen.
Ein Hinweis erst an der Zapfsäule bzw. am Eingang zum Shop ist hingegen zu spät.

Wichtig ist zudem die Angabe der verantwortlichen Stelle, also desjenigen, welcher die personenbezogene Daten erhebt, verarbeitet oder nutzt. Dies ist in der Regel der Tankstellenpächter.

Die Information muss es dem Betroffenen ermöglichen, ohne weitere Recherchen festzustellen, gegenüber wem er wirksam seine Datenschutzrechte insbesondere auf Auskunft oder Löschung geltend machen kann. Hierzu benötigt er Angaben über die Identität der verantwortlichen Stelle, nämlich mindestens den Namen und die postalische Anschrift (Firmenadresse).

Die auf Hinweisschilder anzutreffende Aussage, dass die Überwachung „zu Ihrer und unserer Sicherheit" erfolgt, verärgert hingegen viele Kunden und ist so auch nicht richtig, da der Tankstellenbetreiber nur eigene Zwecke verfolgen kann, nicht aber diejenigen seiner Kunden (welche er darüber hinaus auch nicht für alle kennen kann).

Datenschutzbeauftragte und Vorabkontrolle

Vielen Tankstellenbetreibern ist nicht bekannt, dass gem. § 4d Abs. 5 BDSG eine Vorabkontrolle durchzuführen ist, wenn die Verarbeitung personenbezogener Daten durch die Videoüberwachung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweist. Solche besonderen Risiken liegen regelmäßig vor, wenn Überwachungskameras nicht punktuell, sondern durch die verantwortliche Stelle in größerer Zahl und zentral kontrolliert eingesetzt werden. Ebenso kann die verwendete Technik zu einem solchen besonderen Risiko führen.

Bei Tankstellen sind diese Kriterien meist schon aufgrund der großen Anzahl der eingesetzten Kameras erfüllt, weshalb folglich eine Vorabkontrolle durchzuführen ist, so dass aufgrund der gesetzlichen Regelungen in § 4f Abs. 1 S. 6 BDSG allein deshalb ein betrieblicher Datenschutzbeauftragter zu bestellen ist, da es diesem gemäß § 4d Abs. 6 BDSG obliegt, die Vorabkontrolle vorzunehmen.

Überwachte Bereiche

Bei der Einrichtung der Überwachungskameras ist zu beachten, dass diese nur das Tankstellengelände erfassen und nicht den davor liegenden öffentlichen Bereich (wie Straßen und Wege oder andere Grundstücke).

Im Shop sind viele Kameras regelmäßig so eingestellt, dass diese die Aktivitäten des Personals im Bereich hinter dem Tresen zu umfangreich überwachen.

Eine Videoüberwachung darf gem. § 32 Abs. 1 S. 2 BDSG keine datenschutzrechtlich unzulässige Arbeits- und Leistungskontrolle ermöglichen.

Es kann allenfalls ein berechtigtes Interesse an der Überwachung einzelner Beschäftigter geben, wenn ein begründeter Verdacht auf eine konkrete Straftat besteht und andere Aufklärungsmaßnahmen nicht zur Verfügung stehen bzw. erfolglos geblieben sind. Dann kann die zeitlich begrenzte Videoüberwachung zulässig sein, wenn das Kontrollinteresse den Persönlichkeitsschutz übersteigt. Da diese Voraussetzungen jedoch nicht ständig vorliegen, ist die permanente Überwachung aller Beschäftigten hinter dem Tresen / an der Kasse datenschutzrechtlich unzulässig.

Hier ist seitens des Tankstellenpächters die Kamera so auszurichten, dass nur vor dem Tresen stehende Personen (ggf. also der Tankstellenräuber) erfasst werden, nicht aber der Mitarbeiter dahinter. Unzulässig erfasste Bereiche können bei den meisten Kameras auch verpixelt werden.

Darüber hinaus werden vielfach die in Tankstellen-Shops aufgebauten Stehtische überwacht, zum Teil auch ganze Sitzecken.

Hier fällt die datenschutzrechtlich durchzuführende Interessenabwägung in aller Regel zu Gunsten des Rechts des betroffenen Kunden auf Wahrung seiner informationellen Selbstbestimmung aus.

Dieses Datenschutzgrundrecht verbürgt das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Ob dieses Recht bei einer Videoüberwachung im öffentlich zugänglichen Raum überwiegt, ist einzelfallabhängig und situationsbezogen zu beurteilen. Dabei wächst der Stellenwert der Schutzbedürftigkeit mit zunehmender Bedeutung der Möglichkeit zur individuellen Entfaltung im öffentlichen Raum. So ist die Schutzbedürftigkeit regelmäßig in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, besonders hoch einzustufen. Dies trifft auf die für Kunden eingerichteten Stehtische, durch die ein längerer Aufenthalt in der Tankstelle ermöglicht werden soll, im besonderen Maße zu. Daher werden die Persönlichkeitsrechte der sich hier aufhaltenden Kunden durch eine ständige Videoüberwachung auch erheblich beeinträchtigt.
In solchen Fällen ist der Erfassungsbereich der Kamera daher so zu beschränken, dass unzulässig überwachte Bereiche herausgenommen werden. Auch hier bleibt es dem Tankstellenpächter als verantwortlicher Stelle überlassen, wie dies umgesetzt wird, z.B. durch ein Verschwenken der Kameras oder mittels Verpixeln der unzulässig erfassten Bereiche.

8.7 Private Videoüberwachung als Dauerkonflikt

Die wachsende Zahl von Einbrüchen und Vandalismus weckt auch bei Privatpersonen zunehmend das Bedürfnis, ihr häusliches Umfeld mit Hilfe einer Videoüberwachung (VÜ) schützen zu wollen. Dabei wird regelmäßig nicht bedacht, dass auch eine VÜ des eigenen Grundstücks nur unter bestimmten datenschutzrechtlichen Voraussetzungen rechtskonform ist.
Insbesondere ist eine VÜ grundsätzlich nicht zulässig, sofern auch öffentlich zugänglicher Raum davon betroffen ist.
Aktuell dazu ist auch ein datenschutzrechtliches Kontrollverfahren gegen sog. „Reichsbürger" anhängig.

Zu den Voraussetzungen einer rechtskonformen VÜ durch Privatpersonen ist bereits in der Vergangenheit berichtet worden (s. XX. Tätigkeitsbericht 2009-2010, S. 120).

Auch in den öffentlichen Medien wird vermehrt dieses Thema aufgegriffen. Daher ist im Berichtszeitraum die Anzahl entsprechender ebenfalls Eingaben deutlich angestiegen.

Handhabung von Eingaben

Sofern von einer Petentin/einem Petenten in einer Beschwerde glaubhaft vorgetragen wird, dass eine Nachbarin/ein Nachbar (zumindest auch) öffentlich zugängliche Bereiche videoüberwacht, wird ein datenschutzaufsichtliches Kontrollverfahren eingeleitet.

Dabei wird die sog. verantwortliche Stelle aufgefordert, zu dem von mir verwendeten einschlägigen Fragenkatalog Stellung zu nehmen. Außerdem sind geeignete Unterlagen (z. B. Videografien, Standorte der VÜ-Anlagen, Grundstücksverhältnisse) beizubringen.

Auf dieser Grundlage wird über das weitere Vorgehen entschieden. Dabei wird auch berücksichtigt, dass den Datenschutzaufsichtsbehörden bei Privatpersonen nur eingeschränkte Kontrollbefugnisse (z. B. kein Zutrittsrecht ohne Zustimmung der Grundstückseigentümerin/des Grundstückseigentümers) zur Verfügung stehen.

Die häufig vorgetragene Behauptung, es werde nur eine Attrappe verwendet, kann daher in aller Regel nicht auf ihren Wahrheitsgehalt überprüft werden.

Für den Fall, dass der Sachvortrag einer Petentin/eines Petenten erkennen lässt, dass eine private Stelle neben dem eigenen Grundstück nur das Nachbargrundstück (ohne öffentliche Bereiche) videoüberwacht, werden beide

Parteien über die Rechtslage aufgeklärt und auf den Zivilrechtweg verweisen. Darüber hinaus wird kein Kontrollverfahren eingeleitet.

Reichsbürger nerven nicht nur die Jusitz

Nicht nur für die Justizbehörden in Niedersachsen und die Region Hannover werden die sog. Reichsbürger ein zunehmendes Problem. Auch meine Behörde ist mittlerweile davon betroffen.

So versuchen sich derzeit sog. Reichsbürger, die mit ihrer Videoanlage auch den öffentlich zugänglichen Raum vor ihrem Wohnhaus überwachen, ihrer datenschutzrechtlichen Auskunftspflicht (§ 38 Abs. 3 Satz 1 BDSG) zu entziehen, indem sie

- eine Fülle von Dokumenten zurücksenden, die inhaltlich nichts mit der Fragestellung zur VÜ zu tun haben,
- hiesige Bescheide im Original zurücksenden – versehen mit einem selbst gefertigten Stempel, der einen amtlichen Eindruck erwecken soll,
- eine fadenscheinige Strafanzeige gegen die Sachbearbeiterin stellen.

„Reichsbürger nerven die Justiz" - Kleine Anfrage zur schriftlichen Beantwortung durch die Landesregierung (s. Nds. Landtag - Drucksache 17/5107).

Derartige untaugliche Versuche, die Zusammenarbeit mit der Aufsichtsbehörde zu boykottieren, bleiben jedoch erfolglos.

Im konkreten wie auch ähnlichen Fällen ohne „Reichsbürgerbezug" nutze ich konsequent das zur Verfügung stehende rechtliche Instrumentarium und setze – ggf. auch wiederholt – Zwangsgelder fest, um letztlich die zur Beurteilung des Falles erforderlichen Informationen von der/dem verantwortlichen Kamerabetreiberin/-betreiber zu erwirken.

So bin ich auch im noch nicht abgeschlossenen Fall der „Reichsbürger" vorgegangen.

9. Ordnungswidrigkeiten-Verfahren

9.1 Betretungsrecht der Aufsichtsbehörde: Uneingeschränkter Zugang zu Geschäftsräumen

Wird Mitarbeiterinnnen und Mitarbeitern der Datenschutzaufsichtsbehörde im Rahmen einer Prüfung der Zutritt zu einem Unternehmen verweigert, droht ein Bußgeld. Der vorliegende Artikel erläutert die Rechtslage.

Eine Filiale eines großen Unternehmens sollte von zwei meiner Mitarbeiter auf die Einhaltung datenschutzrechtlicher Vorschriften kontrolliert werden. Allerdings verweigerte der Filialleiter diesen den Zutritt zu den hinteren Geschäftsräumen. Der Leiter hatte von seiner Zentrale die Weisung, dass sich niemand ohne gerichtlichen Beschluss Zugang zu diesen Räumlichkeiten verschaffen dürfe. Aufgrund dieser Weisung half auch eine Verdeutlichung der eindeutigen Rechtslage meinen Mitarbeitern nicht weiter.

Der Auslöser: Videoüberwachung

Zur Vor-Ort-Kontrolle kam es aufgrund einer in der Filiale aufgehängten Videokamera. Das Unternehmen gab mir gegenüber an, dass es sich um eine Attrappe handele. Einem Petenten teilte das Unternehmen hingegen mit, es sei eine echte Kamera.

Wenige Tage später stellte sich bei einem Kontrolltermin heraus, dass es sich tatsächlich um eine batteriebetriebene Attrappe handelte. Auch waren keine Anzeichen für eine Beseitigung etwaiger Beweise erkennbar.

Die Rechtslage

Als Aufsichtsbehörde habe ich gemäß § 38 Abs. 4 Bundesdatenschutzgesetz (BDSG) zur Erfüllung der mir übertragenen Aufgaben ein Zutrittsrecht zu allen Geschäftsräumen. Dabei kann ich Prüfungen und Besichtigungen vornehmen sowie geschäftliche Unterlagen einsehen. Das Unternehmen hat solche Maßnahmen kraft Gesetzes zu dulden.

Zur Durchsetzung dieses Rechts könnten meine Mitarbeiterinnen und Mitarbeiter in dringenden Fällen auch die Polizei hinzuziehen, um sich mit deren Hilfe Zutritt zu verschaffen. Da ein derart dringender Fall nicht vorlag, wurde meinerseits ein Kontrolltermin wenige Tage später schriftlich angeordnet.

Teure Konsequenzen

Die Verweigerung des Zutritts führte dazu, dass noch am selben Tag ein Bußgeldverfahren eingeleitet wurde. Das Unternehmen zeigte sich einsichtig und hat seine Handreichungen für die Filialleitungen entsprechend überarbeitet.

Die Ordnungswidrigkeit war objektiv geeignet, die effektive Arbeit der Aufsichtsbehörde erheblich zu behindern und rechtswidrige Zustände zu verschleiern. Dass dies vorliegend nicht der Fall war, stellte sich erst im Nachhinein heraus. Aufgrund der guten wirtschaftlichen Lage des Unternehmens habe ich daher eine Geldbuße im vierstelligen Bereich festgesetzt. Hierbei war das Einsehen schon bußgeldmindernd berücksichtigt.

9.2 Identitätsverwechselung: Falsche Daten in Auskunftei gespeichert

Bei der Speicherung von Bonitätsinformationen müssen Auskunfteien besonders sorgfältig arbeiten, wie der folgende Bericht verdeutlicht.

Auskunfteien speichern Informationen zur Bonität von u.a. natürlichen Personen. Namensgleichheiten sind dabei eher die Regel als die Ausnahme. Auskunfteien müssen bei der Erfassung von Daten daher ganz besonders auf die richtige Zuordnung von Bonitätsinformationen achten. Eine Zuordnung allein aufgrund des Namens reicht regelmäßig nicht aus.

Im Berichtszeitraum habe ich den Fall einer Verwechslung als Ordnungswidrigkeit verfolgt. Bei Annika M.[1] wurden fälschlicherweise Daten einer Anika M.[1] gespeichert, über mehrere Jahre bereitgehalten und letztlich an ein Kreditinstitut übermittelt. Aufgrund der fehlerhaft gespeicherten Merkmale ergaben sich für die Betroffene Schwierigkeiten bei der Finanzierung.

Rechtslage

Auskunfteien erheben und speichern Daten geschäftsmäßig zum Zweck der Übermittlung. Damit unterliegen sie den besonderen Vorschriften des § 29 BDSG. Die Daten dürfen insbesondere dann bei der Auskunftei gespeichert werden, wenn sie zulässig dorthin übermittelt wurden (§ 28 a BDSG).

Voraussetzung einer zulässigen Speicherung ist zudem die Richtigkeit der Daten, was die Zuordnung zur richtigen Person beinhaltet. Werden Daten innerhalb der Auskunftei dennoch bei falschen Personen gespeichert, so ist diese Speicherung unzulässig. Für die Speicherung falscher Daten besteht keine Rechtsgrundlage.

Zu den Pflichten der Auskunftei gehört auch, dass bei nicht erledigten Sachverhalten spätestens alle vier Jahre zu prüfen ist, ob die Speicherung der Daten noch erforderlich ist (§ 35 Abs. 2 Satz 2 Nr. 4 BDSG). Spätestens hierbei sollten Fehler bei der Zuordnung auffallen.

1 Namen geändert

Konsequenzen für organisatorische Mängel

Bei der Auskunftei konnte ein organisatorisches Verschulden festgestellt werden. Dieses Verschulden war Auslöser der Verwechslung und führte dazu, dass gegen diese Auskunftei ein Bußgeld festgesetzt wurde.

Die Geschäftsführung der Auskunftei hatte keine ausreichenden Aufsichts- und Organisationsmaßnahmen getroffen. Insbesondere wurden wirksame Löschmaßnahmen nicht hinreichend implementiert. Auch die regelmäßig notwendige Überprüfung der manuell erfassten Daten erfolgte nicht.

In der Praxis

Die sogenannte „Einmeldung" durch ein Unternehmen in eine Auskunftei ist z.B. zulässig, wenn die/der Betroffene nach Eintritt der Fälligkeit zweimal schriftlich gemahnt wurde, zwischen der ersten Mahnung und der Einmeldung mindestens vier Wochen liegen, die/der Betroffene auf die bevorstehende Einmeldung frühestens mit der ersten Mahnung hingewiesen wurde und die Forderung nicht bestritten wurde.

Daten bzw. Wahrscheinlichkeitswerte (Score) übermitteln Auskunfteien, wenn Anfragende ihr berechtigtes Interesse an der Kenntnis glaubhaft darlegen und kein Grund zu der Annahme besteht, dass die betroffene Person ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat (§ 29 Abs. 2 Satz 1 BDSG).

Diese Voraussetzungen sind im Fall von Bonitätsabfragen über Privatpersonen regelmäßig nur dann gegeben, wenn für die anfragende Stelle im Rahmen einer sich anbahnenden oder bestehenden Vertragsbeziehung ein finanzielles Ausfallrisiko vorliegt. Sonstige wirtschaftliche Risiken berechtigten grundsätzlich nicht zur Abfrage von Bonitätsauskünften über Privatpersonen.

Nähere Informationen zu Bonitätsauskünften und den Betroffenenrechten können Sie meinem XX. Tätigkeitsbericht ab Seite 45 entnehmen.

9.3 Datenschutzverstoß durch offene E-Mail-Verteiler

Im Berichtszeitraum haben mich wieder einige Fälle offener E-Mail-Verteiler erreicht. Das sind E-Mails die an eine Vielzahl von Empfängern im „An"- bzw. „Cc"-Feld versandt werden, sodass alle Empfänger auch die E-Mail-Adressen der übrigen Empfänger erhalten. Manche dieser Fälle habe ich als Ordnungswidrigkeiten verfolgt. Besonders problematisch ist es, wenn weitere Daten aus den E-Mails hervorgehen.

Häufig nutzen Vereine und kleinere Unternehmen offene E-Mail-Verteiler. Damit offenbaren sie ihren Mitgliedern bzw. Kunden teilweise die gesamte Mitglieder- bzw. Kundendatenbank.

Die Rechtslage: Versand über offene Verteiler nicht erlaubt

Lässt sich eine E-Mail-Adresse einer bestimmten Person zuordnen, handelt es sich um ein personenbezogenes oder zumindest personenbeziehbares Datum (§ 3 Abs. 1 BDSG). Funktions-E-Mail-Adressen wie poststelle@lfd.niedersachsen.de und anonymisierte Adressen haben hingegen keinen Personenbezug.

Beim offenen Verteiler können auch weitere personenbezogene Daten einbezogen sein. Aus der E-Mail könnte sich z.B. ergeben, dass eine bestimmte Dienstleistung in Anspruch genommen wurde oder werden soll (z.B. mit Gesundheitsbezug wie bei der Teilnahme an einer Rückenschule).

Der Versand von E-Mails mit offenem Verteiler stellt eine Übermittlung dar, bei der alle Empfänger die personenbezogenen Daten Dritter erhalten. Eine Einwilligung all dieser Dritter ist zwar denkbar (§ 4 Abs. 1 BDSG), wird jedoch regelmäßig nicht vorliegen. Nach dem datenschutzrechtlichen Grundsatz (Verbot mit Erlaubnisvorbehalt) ist der Versand mit offenen Verteilern daher grundsätzlich nicht erlaubt.

Abschließend ist in jedem Fall zu klären, ob die personenbezogene Adresse allgemein zugänglich ist. In der Praxis bedeutet dies, dass sie z.B. über eine Rückwärtssuche einer gängigen Suchmaschine zu finden sein sollte.

Konsequenzen

Sind E-Mail-Adressen mit Personenbezug nicht allgemein zugänglich, wird ein Ordnungswidrigkeitenverfahren durchgeführt. Das Bußgeld wird gegenüber dem Unternehmen festgesetzt, wenn die Verantwortung für den Verstoß dem Unternehmen zugerechnet werden kann. Ist der Verstoß nicht dem Unternehmen zuzurechnen, kann gegen die oder den jeweiligen Beschäftigten ein Bußgeld verhängt werden.

Sind alle E-Mail-Adressen allgemein zugänglich, wird kein Bußgeldverfahren eingeleitet. Das war im Berichtszeitraum z.B. der Fall, als ein Unternehmen eine E-Mail an personalisierte E-Mail-Adressen diverser kommunaler Körperschaften versandte. Aufgrund ihrer bürgerorientierten Arbeitsweise machten alle Kommunen die E-Mail-Adressen allgemein zugänglich.

Vermeidung von Verstößen

Als einfachste Lösung können Massen-E-Mails als Blindkopie (BCC, Blind Carbon Copy) versandt werden. Die gängigen E-Mail-Programme sorgen dann dafür, dass kein Empfänger die Liste aller Empfänger erhält.

Für manche E-Mail-Programme gibt es auch kleine Zusatzprogramme (sog. Plug-Ins oder Add-Ons), welche die Versendung an eine Vielzahl von An- und Cc-Empfängern verhindern oder zumindest davor warnen.

Ist die Blindkopie keine praktikable Lösung – z.B. weil Blindkopien beim Empfänger oft im Spam-Ordner landen – könnte ein spezialisiertes Mailingprogramm wie GNU Mailman eingesetzt werden. Dabei ist dringend auf eine datenschutzgerechte Konfiguration zu achten; so sollte z.B. nicht jeder Empfänger eine Nachricht über das System verschicken können und auch die übrigen Mitglieder der Liste nicht einsehen können.

9.4 Fehlende Vollmacht: Kontodaten an falsche Empfänger übermittelt

Im Berichtszeitraum sind mir mehrere Fälle zur Kenntnis gelangt, in denen Kontodaten ohne Berechtigung an Dritte übermittelt wurden.

Meist war der Anlass der Übermittlung ein Ehescheidungsverfahren. So haben Ehegatten trotz fehlender Vollmacht Auskunft über Konten des anderen Ehegatten erhalten. In einem Fall wurde hingegen voreilig eine Kontoverbindung von einem Kreditinstitut an eine verbundene Versicherung übermittelt.

Datenschutzrechtlich unzulässig

Handelt es sich nicht um ein Firmenkonto, sind Kontodaten zweifellos personenbezogene Daten. Diese sind sogar besonders schützenswert. Kommen z.B. durch einen Hackerangriff Kontodaten abhanden, hat ein Unternehmen die betroffenen Kunden und die Aufsichtsbehörde darüber umgehend zu informieren (§ 42a BDSG).

Neben den zuständigen Beschäftigten der Bank können auf die Kontodaten grundsätzlich nur der Inhaber des Kontos und ggf. dessen gesetzliche Vertreter zugreifen. Auch Angehörige wie Ehegatten oder Kinder haben zunächst keinen Zugriff. Ein Zugriff ist hingegen über eine Vollmacht möglich. Mit dieser Vollmacht willigt der Kontoinhaber ein, dass auch bestimmte andere Personen auf sein Konto zugreifen dürfen.

Eine Bank ist daher grundsätzlich nicht berechtigt, einem Ehegatten Auskunft über Kontodaten des anderen Ehegatten zu erteilen. Etwas anderes gilt, wenn für den Ehegatten eine entsprechende Vollmacht vorliegt. Dabei kann es vorkommen, dass für manche Konten eine Vollmacht erteilt wird, für andere hingegen nicht.

Zivilrechtliche Verpflichtung bei Ehescheidung

Zwar ist die Auskunft durch die Institute an den anderen Ehegatten unzulässig, wenn keine Vollmacht vorliegt. Das bedeutet jedoch nicht, dass ein Ehegatte dem anderen im Scheidungsverfahren Vermögenswerte verschweigen dürfte.

Im Falle einer Scheidung besteht vielmehr eine familienrechtliche Auskunftspflicht nach § 1379 oder § 1580 BGB. Demnach können die Ehegatten ge-

genseitig Auskunft über das Vermögen des jeweils anderen verlangen. Auch geeignete Belege (z.B. Kontoauszüge) können verlangt werden.

Bei dieser gegenseitigen Auskunftsverpflichtung wird ein Schadenersatzanspruch nach § 7 BDSG gegen ein rechtswidrig handelndes Institut nicht bestehen. Es fehlt bereits an einem Schaden.

Konsequenzen

In einem Fall wurde ein geringes Bußgeld festgesetzt. Das verantwortliche Institut hatte mir die hauseigenen organisatorischen Maßnahmen nicht nachgewiesen, was mich veranlasste, von einem Organisationsverschulden auszugehen.

Konnten die Institute ausreichende organisatorische Maßnahmen nachweisen, wurden keine Bußgelder festgesetzt. Auch gegen die jeweils handelnden Mitarbeiter wurde auf die Festsetzung eines Bußgeldes verzichtet. Bezogen auf einzelne Beschäftigte waren die – jeweils fahrlässig begangenen – Handlungen geringfügig. Das schützt die Beschäftigten allerdings nicht vor Maßnahmen ihrer Arbeitgeber (z.B. Ermahnungen oder Abmahnungen).

9.5 Fragliche Zahlungsfähigkeit: Unzulässiger SCHUFA-Abruf

Der Abruf bei Auskunfteien erfolgt durch Unternehmen typischerweise, um die Zahlungsfähigkeit eines Kunden feststellen zu können. Gelegentlich erfolgen unzulässige Abrufe, bei denen einzelne Beschäftigte des Unternehmens ein ausschließlich privates Interesse an der Auskunft haben.

Oft ist der Hintergrund ein Streit über Schuldentilgung oder bloße Neugier. Einen solchen Fall habe ich im Berichtszeitraum verfolgt. Ein Schwiegervater war sich über die Zahlungsfähigkeit seiner Schwiegertochter wohl im Unklaren, was er mittels Schufa-Abruf klären wollte.

Bekannt wurde der unzulässige Abruf nur, weil die Betroffene eine Selbstauskunft bei der Auskunftei beantragte. In der Selbstauskunft wurde der Arbeitgeber des Schwiegervaters angegeben und der Abruf mit einem beabsichtigten Kauf auf Rechnung begründet. Da es solch einen Kauf nicht gab, wandte sich die Betroffene an mich.

Konsequenzen

Da der Schwiegervater die Schufa-Auskunft durch unrichtige Angaben (vorgeschobener Kauf auf Rechnung) erschlich, beging er eine Ordnungswidrigkeit. Ich habe daher eine Geldbuße gegen ihn festgesetzt. Die Geldbuße fiel verhältnismäßig gering aus, da er die Tat von Anfang an einräumte. Hinzu kam, dass seine wirtschaftlichen Verhältnisse zu berücksichtigen waren, denn er war mittlerweile aus dem Berufsleben ausgeschieden und bezog lediglich eine Rente.

Der unbefugte Abruf aus persönlichem Interesse hätte aber auch erhebliche arbeitsrechtliche Konsequenzen haben können. Gerade in der Finanzbranche, die auf das Vertrauen ihrer Kunden großen Wert legt, bliebe es vielleicht nicht bei einer Abmahnung.

Aber: Wer darf eigentlich abrufen?

Eine Vertragspartnerin / ein Vertragspartner einer Auskunftei darf sich bei dieser nur über die bonitätsrelevanten Umstände einer Person erkundigen, wenn sie ein berechtigtes Interesse hat.

Ein Interesse ist berechtigt, wenn als Zahlungsmethode z.B. „Rechnung“ ausgewählt wird. Unternehmen dürfen sich vergewissern, dass Kunden eine ausreichende Bonität aufweisen, bevor sie eine Zahlungsart akzeptieren, die leicht zum Totalverlust von Ware und Zahlung führen kann.

Ohne ein berechtigtes Interesse ist der Abruf hingegen nicht gestattet. Beispielsweise besteht bei der Zahlung per Vorkasse kein finanzielles Ausfallrisiko, das einen Abruf rechtfertigen würde.

9.6 Folgekosten bei fehlender Antwort der betroffenen verantwortlichen Stelle

Reagiert eine verantwortliche Stelle nicht auf eine Abfrage und ein Kontrollverfahren entstehen zwangsläufig erhebliche Kosten

Ein Petent hatte im Internet eine Bestellung ausgelöst und erhielt am selben Tag eine E-Mail, in der der Verkäufer, die verantwortliche Stelle, einen neuen Premiumservice bewarb. Dieser Service sah mehrere Vorteile für den Kunden vor, u. a. eine zeitlich verkürzte Bearbeitungsdauer für Beanstandungen oder Reklamationen. Der Petent wandte sich an die verantwortliche Stelle, widersprach der werblichen Nutzung seiner Daten und beantragte eine Auskunft über die zu seiner Person gespeicherten Daten, deren Herkunft und mögliche Empfänger dieser Daten.

Nachdem er von der verantwortlichen Stelle keinerlei Antwort erhielt, beschwerte er sich bei mir und bat um Unterstützung.

Nach erster telefonischer Kontaktaufnahme und der Bitte um eine zeitnahe Erstellung der gewünschten Datenschutzauskunft an den Petenten hörte ich auch nach telefonischer und schriftlicher Nachfrage mittels E-Mail nichts mehr. Auch nach offizieller Einleitung eines Kontrollverfahrens erhielt ich keine Rückantwort. Ebenso konnte ich mit der Androhung und der späteren Festsetzung eines Zwangsgelds sowie der Einleitung eines Bußgeldverfahrens das Unternehmen nicht zu einer Reaktion bewegen.

So stellte ich zwar nach einigen Monaten den Eingang des festgesetzten Zwangsgeldes fest, die Beantwortung der von mir gestellten Fragen blieb jedoch weiterhin aus, auch eine Datenschutzauskunft war nicht erteilt worden

Erst nach erneuter Kontaktaufnahme reagierte das Unternehmen endlich und gab die erbetenen Antworten und Auskünfte.

Das gesamte Verfahren zog sich über ein Jahr hin. Letztlich hatte die verantwortliche Stelle neben einem Zwangs- und einem Bußgeld mit den entsprechenden Bearbeitungsgebühren auch die Kosten des Kontrollverfahrens zu tragen.

Insgesamt wurden fast 3.200,-- Euro festgesetzt und gezahlt. Eine zeitnahe Beantwortung der gestellten Fragen hätte der verantwortlichen Stelle unnötigen Aufwand und zusätzlich erhebliche Kosten gespart.

9.7 Statistik Ordnungswidrigkeitenverfahren

Im Berichtszeitraum habe ich 92 Bußgeldverfahren bearbeitet. In diesen Verfahren habe ich 27 Bußgelder über zusammen mehr als 20.000 Euro festgesetzt. Ganz überwiegend wurden die Bußgelder von den Adressaten akzeptiert und bezahlt.

In fünf Fällen habe ich Bußgelder gegen natürliche Personen festgesetzt. Die übrigen 22 Bußgelder habe ich gegenüber Unternehmen verhängt, bei denen mangelhafte organisatorische Vorkehrungen oder Handlungen von Personen mit Leitungsaufgaben zum Verstoß führten.

Konkrete Angaben über die Bußgeldhöhe mache ich nicht öffentlich, um fehlerhafte Deutungen zu vermeiden. 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; anders als bei den hochgradig standardisierten Zuwiderhandlungen im Straßenverkehr.

Fünf Bußgeldverfahren habe ich zudem mit Verwarnungen abgeschlossen. In diesen Fällen waren die datenschutzrechtlichen Verstöße in der Gesamtschau so geringfügig, dass ich von der Festsetzung eines Bußgeldes absehen konnte.

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. Grund war meist, dass eine Verletzung des höchstpersönlichen Lebensbereichs oder der Vertraulichkeit des Wortes (§§ 201, 201a Strafgesetzbuch – StGB) im Raum stand. Eine Abgabe wegen der Verletzung der Vertraulichkeit des Wortes erfolgte beispielsweise, wenn eine Videokamera nicht nur Bilder sondern auch Gespräche aufzeichnete.

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.

Für einen eigenen Strafantrag nach § 44 BDSG hatte ich im Berichtszeitraum keinen Anlass.

10. Aus der Behörde

10.1 Bericht aus dem Datenschutzinstitut Niedersachsen

Wie in den vergangenen Jahren fand auch im Berichtszeitraum für Beschäftigte der öffentlichen Verwaltung eine Reihe von Veranstaltungen in dem zu meiner Behörde gehörenden Datenschutzinstitut Niedersachsen (DsIN) statt.

Der Schwerpunkt meiner Arbeit lag und liegt nach wie vor in der Aufklärung über datenschutzrechtliche Problemlagen und in der Sensibilisierung für datenschutzgerechte Vorgehensweisen. Aus dem Kreis der Teilnehmenden waren im Berichtszeitraum insbesondere Fragen zur Videoüberwachung, zur Nutzung von digitalen Endgeräten und von sozialen Netzwerken von Belang. Durch die Schulungen sollen die Teilnehmenden in die Lage versetzt werden, als Multiplikatorinnen und Multiplikatoren das Datenschutzbewusstsein zu fördern und insbesondere den Beschäftigten vor Ort Lösungsvorschläge, z. B. zum Thema Datensicherheit, anbieten zu können.

Der Grundkurs „Einführung in das Datenschutzrecht“ sowie die Kurse „Basiswissen für behördliche Datenschutzbeauftragte“ und „Datenschutz in Schulen“ sind am stärksten nachgefragt. Wie in den Jahren zuvor sind zudem weitere Veranstaltungen mit Schwerpunktthemen (Personaldatenschutz, Sozialdatenschutz, sowie Themen aus dem technisch-organisatorischen Bereich) angeboten worden. Zusätzlich konnte im Berichtszeitraum ein weiteres Fortbildungsangebot realisiert werden, das sich mit der Videoüberwachung öffentlicher Stellen und der damit verbundenen Vorabkontrolle befasst. Der Bedarf für dieses Kursangebot hat sich insbesondere aus Beratungsgesprächen bei den öffentlichen Stellen ergeben. Daneben wurden sowohl im kommunalen als auch im Bereich des Justizministeriums Inhouse-Veranstaltungen zum Thema „Einführung in das Datenschutzrecht“ durchgeführt. Die Forderung der Teilnehmenden aus den vergangenen Jahren, den Erfahrungsaustausch der behördlichen Datenschutzbeauftragten nicht in voneinander unabhängige Veranstaltungen für die Kommunal- und Landesverwaltung aufzuteilen, zeigt, dass es in Niedersachsen eine enge Vernetzung der digitalen Verwaltung gibt.

Von allen Teilnehmenden wurden erste Hinweise zur europäischen Datenschutzreform mit Interesse zur Kenntnis genommen und umfassende Schulungsangebote zu den neuen Rechtsvorschriften gefordert.

10.2 IT-Labor der LfD: Investition in moderne Analysetechnik

Die Digitalisierung unserer Gesellschaft schreitet immer schneller voran und dringt verstärkt auch in das persönliche Umfeld der Bürgerinnen und Bürger vor. Die Nutzung von Smartphones, Apps, Smart-TVs, Wearables und digitalen Assistenten ist aus unserem Alltag nicht mehr wegzudenken. Digitale Dienste und Produkte haben unsere Kommunikation und die Arbeitswelt genauso wie die Freizeitgestaltung in den vergangenen zehn Jahren stark verändert. Aus diesem Grund hat sich die LfD bereits im Jahr 2015 dazu entschieden, ein IT-Labor aufzubauen und in entsprechende Technik und Personal zu investieren.

Im Laufe des Jahres 2016 wurde so die Möglichkeit geschaffen, Produkte und Dienstleistungen wie z.B. Apps, Wearables oder Websites zu analysieren. Damit wird es bereits jetzt und zukünftig noch besser möglich, datenschutzrechtliche Fragestellungen sowohl mit rechtlichem als auch technischem Know-how zu beurteilen.

Ausstattung des Labors: State of the Art

Die Qualität eines Labors hängt im Wesentlichen von zwei Faktoren ab: einer aktuellen technischen Ausstattung und dem Sachverstand des vorhandenen Personals.

Im Jahr 2016 konnte die bereits 2015 beantragte und genehmigte Stelle für das IT-Labor mit einem promovierten Informatiker besetzt werden. Auf Basis des von ihm erarbeiteten Konzeptes konnte unter Nutzung des vorhandenen Investitionsbudgets die Grundausstattung des IT-Labors mit Soft- und Hardware im Jahr 2016 beschafft werden.

Um das IT-Labor zukünftig bei möglichst vielen verschiedenen Prüfszenarien einsetzen zu können, wurde bei jeder einzelnen Beschaffung darauf geachtet, dass die Hard- und Software so ausgewählt wurde, dass eine möglichst hohe Variabilität im Hinblick auf mögliche zukünftige Prüfungen erreicht wird.

Im Bereich Hardware wurden sowohl ein Desktoprechner, als auch Laptops und ein Standardrouter beschafft. Die Rechner wurden so konfiguriert, dass sie unter den Betriebssystemen von Microsoft (Windows in verschiedenen Versionen), Apple und verschiedenen Linux-Varianten (Kali-Linux und Ubuntu) betrieben werden können. Mit dieser Konstellation können über 95% der in Niedersachsen verwendeten Systeme abgebildet werden.

Mobile Endgeräte (Smartphones) wurden für die marktbeherrschenden Betriebssysteme iOS (i-Phone 7) und Android (Nexus 6P) beschafft. Auf diesen werden dann die zu prüfenden Apps installiert.

Software: Zur Virtualisierung von Systemen wird das Produkt von VMware (WorkstationPro) sowie VirtualBox eingesetzt. Mit der BurpSuite von Portswigger wurde zudem ein erstes leistungsfähiges Analysetool erworben, das bei der Auswertung von Websites und von Apps auf Smartphones zum Einsatz kommen kann.

Mit Hilfe dieses Tools ist es z.B. möglich, trotz verschlüsselter Kommunikation (https) zwischen Server und Client / App die übertragenen Inhalte auszuwerten.

Zusätzlich wurden für ein erstes Prüfprojekt mehrere Wearables unterschiedlicher Hersteller erworben.

Das IT-Labor ist nach Beschaffung der Grundausstattung einsatzfähig. Für spezielle Prüfprojekte müssen allerdings jeweils die zu prüfenden Geräte, Produkte bzw. Software / Apps beschafft werden. Ebenso muss die vorhandene IT-Labor-Ausstattung bei Bedarf aktualisiert werden, um so für die zukünftigen Entwicklungen in der digitalen Welt gerüstet zu sein.

Einsatzszenarien

Analyse von Software und Daten

Auf den vorhandenen Laborrechnern (Desktop-Rechner, Laptop, Smartphones, Tablets) können Analysen erfolgen, bei denen untersucht wird, wie Daten durch die vorhandenen Betriebssysteme oder die auf den Systemen installierte Software bzw. Apps verarbeitet werden. Diese Analyse erfolgt dabei ohne Kommunikation mit anderen Rechnern oder über das Internet.
Das Ergebnis dieser Analysen zeigt auf, was die Software bzw. die Apps verursachen, welche Daten verarbeitet werden und wo und wie (verschlüsselt oder unverschlüsselt) diese abgelegt werden.

Prüfung des Kommunikationsverhaltens

Neben der Frage, welche Daten verarbeitet werden, ist die Frage, welche Daten in welcher Form an wen übermittelt werden, datenschutzrechtlich ebenfalls von besonderer Bedeutung.
Die Analyse der Kommunikation von Systemen, Websites, Programmen und Apps mit anderen Systemen, (sei es über eine direkte Verbindung innerhalb des IT-Labors oder über die vorhandene DSL-Leitung mit Systemen, die über das Internet erreichbar sind), kann in dem IT-Labor der LfD ebenfalls durchgeführt werden.

Das Ergebnis dieser Analysen zeigt, wer die Daten erhält (d.h. welcher Rechner, physikalisch durch die IP-Adresse beschrieben) und welche Daten übermittelt werden (z.B. Standortdaten, Passwörter, Kontodaten oder technische Informationen wie Browserkennung, Fingerprinting oder Website Tracking Informationen).

Dabei ist zu beachten, dass es nicht immer möglich ist, eine Verschlüsselung zu umgehen oder aufzubrechen und dadurch den übermittelten Inhalt transparent zu machen.

Analyse von über das Internet erreichbaren Systemen

Im Rahmen der aufsichtsrechtlichen Tätigkeit der LfD können auch IT-Systeme von Unternehmen und Behörden geprüft werden.

Soll diese Prüfung nicht anlassbezogen und daher ohne Kenntnis der Prüfenden durchgeführt werden, so besteht durch den Einsatz des IT-Labors die Möglichkeit, über das Internet die IT-Systeme der zu Prüfenden zu analysieren.

Das Ergebnis dieser Analysen kann unter bestimmten Bedingungen aufzeigen, ob und wie die Systeme bzw. der Zugang zu den Systemen gesichert ist, welche Hard- und Software in welcher Version verwendet wird und welche Verschlüsselungen ggf. verwendet werden. So ist es z.B. in vielen Fällen möglich festzustellen, ob das IT-System immer noch für die Heartbleed-Schwachstelle anfällig ist.

Ein aktives Überwinden von vorhandenen Sicherheitsmechanismen sowie der unerlaubte Zugriff auf gespeicherte Daten sind allerdings nicht vorgesehen.

10.3 Das Standard-Datenschutzmodell

Bereits in meinen vorigen Tätigkeitsberichten habe ich es dargestellt: Aus der Notwendigkeit zur Modernisierung der datenschutzrechtlichen Schutzziele hat sich die Erkenntnis entwickelt, dass es einer systematischen, transparenten und überprüfbaren Vorgehensweise bedarf, um die geeigneten technischen und organisatorischen Maßnahmen zu bestimmen, die zur Gewährleistung eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten erforderlich sind. So war es zusätzlich zur Benennung und Definition der aus dem Datenschutzrecht abgeleiteten Gewährleistungsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettung, Transparenz und Intervenierbarkeit)[1] geboten, mit dem Standard-Datenschutzmodell (SDM) eine für Verantwortliche und Aufsichtsbehörden gleichermaßen taugliche Methodik zu entwickeln[2]. Eine - nicht zuletzt vor dem Hintergrund der europäischen Datenschutzreform - anspruchsvolle Aufgabenstellung.

Nach intensiver Vorarbeit in den Vorjahren kamen rund 70 Juristen und Techniker der Datenschutzbehörden am 29.04.2015 zu einem Workshop „SDM – der Weg vom Recht zur Technik“ in Hannover zusammen, um diesen Prototyp in einem größeren Rahmen vorzustellen und zu diskutieren. Entlang der einzelnen Vorträge entspann sich eine angeregte Diskussion, die sowohl den breiten Konsens, dass es eines entsprechenden Modells dringend bedarf, als auch die Notwendigkeit zur Nachbesserung und Ergänzung in einzelnen Teilbereichen aufzeigte. Am meisten vermisst wurde der als Anhang konzipierte, jedoch noch nicht in Angriff genommene Katalog mit Standard-Datenschutzmaßnahmen (Maßnahmenkatalog), der analog zu den BSI-Grundschutzkatalogen die zusätzliche Auswahl speziell datenschutzrechtlich erforderlicher Sicherungsmaßnahmen ermöglicht.

1 „Ein modernes Datenschutzrecht für das 21. Jahrhundert - Eckpunkte“, verabschiedet von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, Kapitel 3 „Technischer und organisatorischer Datenschutz“: S. 18-20
http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.html?nn=408908
und 21. Tätigkeitsbericht der LfD Niedersachsen 2011-2012: „Schutzziele statt Kontrollziele“: S. 100-101
https://www.lfd.niedersachsen.de/startseite/allgemein/taetigkeitsberichte/2011_2012/14122011-133624.html

2 22. Tätigkeitsbericht der LfD Niedersachsen 2013-2014: „Das Standard-Datenschutzmodell nimmt Konturen an“: S. 184-186
https://www.lfd.niedersachsen.de/startseite/allgemein/taetigkeitsberichte/informationssicherheit_tkue_privacy_by_design_kameras_thiel_stellt_22_taetigkeitsbericht_20132014_vor/14122011-139039.html

Diskurs und Weiterentwicklung sollten jedoch nicht nur im Kreis der Datenschutzbehörden stattfinden, sondern auch in die Fachöffentlichkeit hineingetragen werden.

- So erfolgte ebenfalls im Frühjahr 2015 eine erste Vorstellung des Modells auf der 16. Sitzung des IT-Planungsrates (IT-Koordinierung von Bund und Ländern).

- Die Inhalte des internen SDM-Workshops vom 29.04.2015 wurden in einem Tagungsband zusammengefasst und veröffentlicht.[3]

- Im Oktober 2015 wurde die Version 0.9 des SDM von der DSK zustimmend zur Kenntnis genommen und bewusst noch im „Entwurfsstadium" zur Beförderung einer umfassend angelegten Diskussion zur Veröffentlichung auf den Webseiten der Datenschutzbehörden freigegeben.

Zur Vorstellung und Etablierung des Modells auf europäischer Ebene galt es zudem, die Anforderungen der nach fast vierjähriger Verhandlung vom Europäischen Parlament am 14.04.2016 angenommenen endgültigen Fassung der EU-Datenschutzgrundverordnung (DS-GVO) einzuarbeiten.

Nach Abschluss dieser arbeitsintensiven Anpassungen hat im November 2016 die DSK der Version 1.0 des SDM sowie dem noch nicht abgestimmten Entwurf der ersten 16 Bausteine des Maßnahmenkatalogs zugestimmt. Die nunmehr von der „Entwurfs"- zur „Erprobungsfassung" weiter entwickelte Methode[4] soll sowohl in der eigenen Kontroll- und Beratungspraxis als auch bei der Planung und beim Betrieb von Datenverarbeitungen durch verantwortliche Stellen im öffentlichen und nicht-öffentlichen Bereich getestet werden. Eine laufende Fortentwicklung ist ausdrücklich erwünscht.

Zum Ende des Berichtszeitraums war geplant, dass die Bausteine des Maßnahmenkatalogs im Laufe des Jahres 2017 durch den AK Technik endabgestimmt und ebenfalls zur Veröffentlichung freigegeben werden. Ich werde in den nächsten Tätigkeitsberichten über die weiteren Fortschritte informieren.

3 Tagungsband „Das Standard-Datenschutzmodel – der Weg vom Recht zur Technik"
https://www.lfd.niedersachsen.de/startseite/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/standarddatenschutzmodell/standard-datenschutzmodell-139069.html

4 „Das Standard-Datenschutzmodell - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele" V.1.0 – Erprobungsfassung
https://www.lfd.niedersachsen.de/startseite/technik_und_organisation/orientierungshilfen_und_handlungsempfehlungen/standarddatenschutzmodell/standard-datenschutzmodell-139069.html