Unterrichtung

Der Niedersächsische Ministerpräsident Hannover, den 26.05.2016

Herrn
Präsidenten des Niedersächsischen Landtages

Hannover

Sehr geehrter Herr Präsident,

als Anlage übersende ich die

> **Stellungnahme der Landesregierung zum XXII. Bericht über die Tätigkeit der Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 2013 und 2014** (Drs. 17/4650).

Federführend ist das Ministerium für Inneres und Sport.

Mit freundlichen Grüßen

Stephan Weil

Stellungnahme der Landesregierung zum XXII. Bericht über die Tätigkeit der Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 2013 und 2014

Vorbemerkungen

Der Tätigkeitsbericht (TB) der Landesbeauftragten für den Datenschutz Niedersachsen (LfD) für die Jahre 2013 - 2014 befasst sich in gewohnter Aufteilung mit dem Datenschutz für den öffentlichen Bereich, den nicht öffentlichen Bereich (Wirtschaftsbereich) und den übergreifenden Bereich des technisch-organisatorischen Datenschutzes. Hinzu kommen besondere Themen sowie der Bereich des Datenschutzes in Europa und im internationalen Datenverkehr. Ein besonderes Augenmerk gilt der Europäischen Datenschutzreform, über die im Zusammenhang mit einzelnen Themen bereits im letzten Tätigkeitsbericht und der Stellungnahme der Landesregierung berichtet wurde. Sowohl die Datenschutz-Grundverordnung wie auch die Datenschutzrichtlinie für den Bereich der Polizei und Justiz werden nunmehr voraussichtlich Mitte des Jahres 2016 in Kraft treten und nach zwei Jahren in den Mitgliedstaaten anzuwenden sein.

Gemäß § 22 Abs. 3 Satz 1 des Niedersächsischen Datenschutzgesetzes (NDSG) ist der Bericht für den Datenschutz im öffentlichen Bereich dem Landtag jeweils für zwei Kalenderjahre vorzulegen; die Landesregierung nimmt hierzu gegenüber dem Landtag innerhalb von sechs Monaten Stellung. Die Verpflichtung der LfD zur Berichterstattung über Prüfungen im nicht öffentlichen Bereich ergibt sich aus § 38 Abs. 1 Satz 7 Bundesdatenschutzgesetz (BDSG). Eine Stellungnahme der Landesregierung ist hierzu gesetzlich nicht vorgesehen. Für diesen Bereich wird daher - wie in den vergangenen Berichtszeiträumen - nur zu einzelnen ausgewählten Themen von besonderem Interesse oder bei ausdrücklicher Kritik der LfD Stellung genommen.

Im Impressum des Tätigkeitsberichts erfolgt folgender Hinweis: „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."

Die maskuline Personenbezeichnung als Oberbegriff für Frauen und Männer führt dazu, dass Frauen „mitgemeint" sein sollen. Dieser Umstand wird von hier kritisch gesehen. Es sollten Personenbezeichnungen gewählt werden, die Frauen in der Sprache stärker „sichtbar" machen. Parallelbezeichnungen für beide Geschlechter behindern aus Sicht der Landesregierung auch nicht die Lesbarkeit des Berichts; außer Parallelformulierungen können beispielsweise auch Personenbezeichnungen weniger oft wiederholt, Personenbezeichnungen umschrieben oder geschlechtsneutrale Personenbezeichnungen gewählt werden.

Das Gesetz zur Förderung der Gleichstellung der Frau in der Rechts- und Verwaltungssprache vom 27.02.1989 (Nds. GVBl. S. 50) sowie der Beschluss des Landesministeriums über die Grundsätze für die Gleichbehandlung von Frauen und Männern in der Rechtssprache vom 09.07.1991 (Nds. MBl. S. 911) verlangen, dass in Rechts- sowie Verwaltungsvorschriften des Landes sowie in der Rechtssprache allgemein im Regelfall beide Geschlechter benannt werden sollen. Dieser Grundsatz ist auch auf Veröffentlichungen des Landes Niedersachsen anwendbar.

Dieser Hinweis wurde bereits in der Stellungnahme der Landesregierung vom 06.10.2015 zum XXI. Tätigkeitsbericht gegeben. Leider hat er in dem aktuellen Bericht teilweise keine Berücksichtigung gefunden. Daher wird erneut angeregt, diesen Hinweis nunmehr beim nächsten Tätigkeitsbericht vollständig zu berücksichtigen.

Globale Überwachung durch Geheimdienste

(TB, Seiten 12 bis 15)

Der Tätigkeitsbericht greift die massenhafte Datenerhebung durch die NSA und andere westliche Geheimdienste auf (Stichworte: NSA, Snowden, PRISM, TEMPORA und XKEYSCORE). In den Konferenzen der Datenschutzbeauftragten des Bundes und der Länder wurde dies mehrfach thematisiert und mündete in eine Reihe von Entschließungen:

- Es dürfe keine anlasslose umfassende Überwachung durch Nachrichtendienste geben.

- Dazu gehöre nationales, europäisches und internationales Recht, das einen umfassenden Schutz der Privatsphäre und informationellen Selbstbestimmung sicherstellt.
- Eine effektive Kontrolle der Nachrichtendienste sei sicherzustellen.
- Auch technisch-organisatorisch müsse die informationelle Selbstbestimmung stärker geschützt werden: kryptographische Verfahren zur elektronischen Kommunikation sollten verstärkt eingesetzt und weiterentwickelt werden; die IT-Sicherheit soll insofern verbessert werden; Geolokalisierung sollte eingeschränkt werden, Cloud Computing nur von vertrauenswürdigen Unternehmen genutzt werden.

Die im parlamentarischen Beratungsprozess befindliche Novelle des Niedersächsischen Verfassungsschutzgesetzes (NVerfSchG) sowie die Geschäftsordnung des Niedersächsischen Landtags setzen die oben genannten Entschließungswünsche nach mehr Transparenz, strengerem gesetzlichen Schutz des Rechts auf informationelle Selbstbestimmung und stärkerer Kontrolle des Verfassungsschutzes konsequent um:

– Transparenz soll in einem novellierten NVerfSchG durch eine verstärkte Kontrolle auf unterschiedlichen Ebenen erreicht werden: beginnend mit Dokumentations- und Berichtspflichten gegenüber dem parlamentarischen Kontrollgremium, der G10-Kommission und der LfD, über zahlreiche Mitteilungspflichten gegenüber Betroffenen sowie Auskunftsrechte.

– Die Kontrollmöglichkeiten des Ausschusses für Angelegenheiten des Verfassungsschutzes (AfAV) im Landtag und der G10-Kommission werden verstärkt:

  – Die Unterrichtung des AfAV wird stärker gesetzlich verankert.

  – Die Rechte des AfAV werden gestärkt, insofern als die Rechte zur Bestellung von Sachverständigen und zur Beteiligung von Mitarbeiterinnen und Mitarbeitern der Fraktionen ausgeweitet werden.

  – Es wird eine Regelung für Beschäftigte der Verfassungsschutzabteilung geschaffen, die es ihnen ermöglicht, sich auch an einzelne Mitglieder des AfAV zu wenden. Damit wird die dienstwegunabhängige, externe Kontrollmöglichkeit verstärkt.

  – Die G10-Kommission ist nunmehr auch in den Entscheidungsprozess zum Einsatz besonders eingriffsintensiver nachrichtendienstlicher Mittel eingebunden.

– Die Kontrolldichte durch den Landtag erhöht sich dadurch, dass sowohl der AfAV als auch die G10-Kommission gesetzlich verpflichtet sind, einmal jährlich über ihre Tätigkeit zu berichten.

– Die Kontrollbefugnisse durch die LfD werden hinsichtlich der Zustimmung zur Nichtbenachrichtigung erweitert. Darüber hinaus wird den Kontrollbefugnissen der LfD dadurch noch mehr Gewicht verliehen, als sie den AfAV auch über Sachverhalte außerhalb ihres sachlichen Zuständigkeitsbereichs informieren soll (§ 25 Abs. 6). Auch Beanstandungen, die nur zufällig entdeckt werden, unterliegen daher einer grundsätzlichen Berichtspflicht, was die Kontrolldichte über die Verfassungsschutzbehörde erhöht.

– Die rechtlichen Folgerungen aus dem Urteil des Bundesverfassungsgerichts zum Antiterrordateigesetz werden mit der Gesetzesnovelle ebenfalls umgesetzt. Dies betrifft vor allem die Übermittlungsbefugnisse und die Datenerhebung zu sogenannten Kontakt- oder Begleitpersonen.

Darüber hinaus stehen sämtliche interne Dienstvorschriften, die Datenverarbeitungsprozesse und die IT-Sicherheit betreffen, auf dem Prüfstand, sodass auch in dieser Hinsicht eine Reaktion auf die Entschließungen der Datenschutzbeauftragten erfolgen wird.

Hinsichtlich der vom Tätigkeitsbericht ebenso aufgegriffenen NSU-Untersuchungsausschüsse ist aus Sicht der Verfassungsschutzbehörde zu berichten, dass seitens des Fachbereichs Rechtsextremismus umfangreiche Zulieferungen an NSU-Untersuchungsausschüsse auf Bundes- und Landesebene geleistet wurden und werden. Hiermit wird ein eigener Beitrag zur weiteren Aufklärung des NSU-Skandals geleistet. Auch dies steht unter dem weitgehenden Gedanken der parlamentarischen Kontrollmöglichkeit und Transparenz nachrichtendienstlichen Handelns.

Hinsichtlich der Entschließung der Datenschutzbeauftragten zur Stärkung der IT-Sicherheit ist anzumerken, dass die Verfassungsschutzabteilung ihre Informationstechnik fortwährend erneuert: Projekte wie der Anschluss an den Niedersachsen-Client (NIC), die Einsetzung eines Dokumentenmanagementsystems und die Neuverkabelung im Hause seien hier beispielhaft genannt.

Die im Tätigkeitsbericht angesprochene strategische Auslandsüberwachung liegt im Zuständigkeitsbereich des Bundes.

„Mindestspeicherfrist“ statt Vorratsdatenspeicherung

(TB, Seiten 16 bis19)

Basierend auf dem Urteil des Bundesverfassungsgerichts vom 02.03.2010 beschreibt die LfD in ihrem Bericht die Entwicklungen und die rechtspolitische Diskussion um die Speicherfristen von Verkehrsdaten von Telekommunikationsanschlüssen und stellt die Gefahren einer anlasslosen Vorratsdatenspeicherung dar.

Aus Sicht der Landesregierung müssen den Sicherheitsbehörden diejenigen Maßnahmen, die für eine effektive Strafverfolgung und Gefahrenabwehr sowie zur Verhinderung von rechtsfreien Räumen notwendig sind, zur Verfügung stehen. Hierunter fällt die Mindestspeicherfrist bestimmter Verkehrsdaten.

Mit dem vom Deutschen Bundestag am 16.10.2015 beschlossenen „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“ werden Telekommunikationsunternehmen, Internetprovider und andere Zugangsanbieter verpflichtet, bestimmte Verkehrsdaten für einen festgelegten Zeitraum zu speichern.

Geschwindigkeitsabschnittsüberwachung „Section Control“

(TB, Seiten 20 bis 22)

Zentraler Bestandteil der Verkehrssicherheitsstrategie der niedersächsischen Polizei im Rahmen ihrer Verkehrssicherheitsinitiative (VSI) 2020 ist die Überwachung der zulässigen Höchstgeschwindigkeit, die nachweislich einen erheblichen Einfluss auf die Abnahme von Unfallhäufigkeit und -schwere hat. Für längere Straßenabschnitte mit einer signifikanten Häufung schwerer, geschwindigkeitsbedingter Unfälle ist die punktuelle Überwachung jedoch nur bedingt geeignet, da die Unfälle sich häufig auf einem mehrere Kilometer langen Streckenabschnitt verteilen. In der Konsequenz müssten mehrere stationäre oder mobile Überwachungsgeräte positioniert werden.

Für längere Straßenabschnitte steht inzwischen jedoch eine Technik zur Verfügung, die Verkehrsteilnehmerinnen und Verkehrsteilnehmer zu einer gleichmäßigen, unfallpräventiven Fahrweise veranlasst: die sogenannte Abschnittüberwachung der Geschwindigkeiten, umgangssprachlich auch Section Control genannt, mit der das Durchschnittstempo sämtlicher Fahrzeuge auf einer Wegstrecke gemessen werden kann.

Am 01.09.2014 hat das Ministerium für Inneres und Sport (MI) bekannt gegeben, diese Technik, die in Deutschland noch nicht zugelassen ist, in Niedersachsen in einem Pilotprojekt zu testen.

In die Planungen zur Einführung dieses Projektes wurde die LfD frühzeitig eingebunden, deren Rechtsauffassung zur Rechtsgrundlage und zu den Rahmenbedingungen eines solchen Pilotprojektes wie folgt mitgeteilt wurde: Es gebe zurzeit keine Rechtsgrundlage für den Einsatz von Section Control. Angesichts der Tatsache, dass in Niedersachsen zunächst zu Erprobungszwecken eine Section Control-Anlage (als Pilot) eingeführt werden soll, worauf die Verkehrsteilnehmerinnen und Verkehrsteilnehmer am Einsatzort unübersehbar hingewiesen werden sollten, werde es für vertretbar gehalten, dass die Polizei eine solche Anlage im öffentlichen Verkehrsraum zu Erprobungszwecken unter bestimmten, im Tätigkeitsbericht genannten Voraussetzungen einsetzt. Danach besteht Einvernehmen mit der LfD, dass der Einsatz der Streckenüberwachungsanlage Section Control in der Erprobungsphase unter Beachtung der dargestellten Grundsätze zulässig ist.

Dies ist unabhängig davon, ob nach Auffassung des MI die Generalbefugnis des § 11 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung als Rechtsgrundlage herange-

zogen werden kann oder angesichts der oben zitierten Rechtsauffassung der LfD aus dem Jahr 2014 der Betrieb der Anlage ohne spezielle Rechtsgrundlage zu Erprobungszwecken vertretbar ist.

Das MI teilt darüber hinaus auch die Auffassung der LfD insoweit, als dass der dauerhafte Einsatz der Anlage erst möglich ist, wenn durch den Gesetzgeber eine spezielle Rechtsgrundlage geschaffen wird.

Zwischenzeitlich ist das Verfahren zum Betrieb der Überwachungsanlage Section Control weiter fortgeschritten. Die am Ende des Berichtszeitraums noch nicht vorliegenden Unterlagen, insbesondere das Datenschutzkonzept, wurden der LfD im Sommer 2015 übergeben und anschließend erläuternde Gespräche geführt sowie schriftliche Stellungnahmen ausgetauscht. Der abschließend von der LfD formulierte Ergänzungsbedarf für das Datenschutzkonzept wird derzeit abgearbeitet.

Obwohl auch nach Auffassung der LfD diese ergänzenden Details sich nicht einführungsverhindernd auf die Pilotphase auswirken, sollen auch diese Anforderungen des Datenschutzes an die neue Verkehrsüberwachungstechnik bereits für die Pilotphase berücksichtigt werden.

Verfassungsschutz im Auftrage des Landtags kontrolliert

(TB, Seite 23)

Gemäß § 27 Abs. 1 Satz 1 NVerfSchG hat der Ausschuss für Angelegenheiten des Verfassungsschutzes des Niedersächsischen Landtages die LfD beauftragt, die Speicherung diverser personenbezogener Datensätze in der Verfassungsschutzbehörde auf ihre Rechtmäßigkeit zu überprüfen. Der Bericht der LfD geht auf die Problempunkte in diesem Zusammenhang ein, wie bereits durchgeführte Datenlöschungen und die Unzulässigkeit von Speicherungen, da die Voraussetzungen der zugrunde gelegten Eingriffsnormen nicht erfüllt waren.

Auf die Feststellungen des Berichtes hat die Verfassungsschutzbehörde durch einen umfassenden Reformprozess reagiert mit der zuvor dargestellten Gesetzesnovelle, der Überarbeitung sämtlicher Dienstvorschriften und dem Erlass temporärer Verfügungen bis zur endgültigen Umsetzung der Reform.

Projekte zur Überwachung der Telekommunikation (TKÜ) bei der Polizei

(TB, Seiten 27 bis 30)

Die LfD knüpft an ihren Bericht für die Jahre 2011 und 2012 an und beschreibt die aus ihrer Sicht weiterhin bestehenden Defizite bei der TKÜ.

Vor dem Hintergrund der rasanten technischen Entwicklung und der zunehmenden Verlagerung der Telekommunikation auf das Internet besteht weiterhin das dringende Erfordernis, die Instrumente für die Erkenntnisgewinnung der Sicherheitsbehörden den veränderten Gegebenheiten anzupassen. Kommunikation wird durch die technischen Entwicklungen der nächsten Jahre in wesentlich stärkerem Maße internetbasiert, mobil, verschlüsselt, unter Nutzung internationaler Anbieter und Strukturen und mit wesentlich höherem Datenaufkommen stattfinden. Dabei sind auch weiterhin die Aspekte des Datenschutzes mit hoher Priorität zu berücksichtigen.

Die von der LfD beschriebenen Mängelpunkte werden, soweit technisch und fachlich umsetzbar, durch das Landeskriminalamt Niedersachsen in einem kontinuierlichen Dialog mit der LfD weiterhin priorisiert betrachtet und bearbeitet. Die Abhängigkeit vom Dienstleister der Systemtechnik zur TKÜ ist hierbei in weiten Teilen maßgeblich. Letztmalig fand am 12.02.2016 ein entsprechendes Gespräch statt. Dabei wurde u. a. vereinbart, die Mängelliste in einem abgestimmten Verfahren möglichst zeitnah einvernehmlich abzuarbeiten.

Zudem ist vorgesehen, dass mit dem Aufbau des geplanten Rechen- und Dienstleistungszentrums Polizei im Verbund der norddeutschen Küstenländer ab Frühjahr 2016 der Dialog weiter intensiviert wird und vor diesem Hintergrund die spezifischen Aspekte des Datenschutzes im Zusammenhang mit der Telekommunikationsüberwachung zielgerichtet berücksichtigt werden.

Neues Bundesmeldegesetz

(TB, Seiten 31 bis 32)

Der Bericht der LfD befasst sich auch mit den Entwicklungen im Melderecht. Mit dem Bundesmeldegesetz (BMG) wurden - anders als im Bericht dargestellt - nicht nur die geltenden Meldegesetze der Länder ersetzt, sondern auch das Melderechtsrahmengesetz abgelöst.

Die Sicherstellung der neu geregelten Verpflichtung, den in § 34 Abs. 4 Satz 1 BMG aufgezählten Behörden zu jeder Zeit Melderegisterdaten zum automatisierten Abruf bereitzuhalten, wird durch den Landesbetrieb IT.Niedersachsen (IT.N) wahrgenommen. Insoweit werden die Kommunen entlastet, die technischen Voraussetzungen zu schaffen und bereitzuhalten, um einen jederzeitigen automatisierten Abruf zu gewährleisten. Dafür hat das Land Niedersachsen bei IT.N einen Melderegisterdatenspiegel errichtet. Um die über 400 kommunalen Meldebehörden von der Verpflichtung zum Vorhalten der Daten zu jeder Zeit zu entlasten, werden die Meldedaten der kommunalen Meldebehörden in den Melderegisterdatenspiegel gespiegelt und zum Abruf bereitgehalten.

Reisegewerbekarte

(TB, Seite 37)

Der Tätigkeitsbericht befasst sich mit der Zulässigkeit der Datenübermittlung in Antragsverfahren auf Ausstellung einer Reisegewerbekarte an die Industrie- und Handelskammern (IHKn) und die Handwerkskammern (HWKn).

Die Rechtsgrundlagen einschlägiger Datenübermittlungen wurden zwischen der LfD und dem Ministerium für Wirtschaft, Arbeit und Verkehr (MW) erörtert. Anlass hierfür war die einzige bis heute bekannte Übermittlung. Auch auf Nachfrage konnten Anhaltspunkte dafür, dass es sich um eine Regelübermittlung bzw. mehrfach praktizierte Übermittlung handele, nicht gewonnen werden.

Die LfD und MW stimmten darüber überein, dass es für entsprechende Datenübermittlungen keine Rechtsgrundlage gibt. Da von Seiten der IHKn und der HWKn in der Vergangenheit sowie bei Erörterung der Nachfrage der LfD ein Interesse vorgetragen wurde, eine einschlägige Rechtsgrundlage zu schaffen, wurde dieser Bedarf in der Frühjahrssitzung 2014 des Bund-/Länderausschusses „Gewerberecht“ erörtert. Der Bund-/Länderausschuss entschied mehrheitlich, dass - wie auch vom MW festgestellt - die Gewerbeordnung keine Rechtsgrundlage für eine Datenübermittlung enthält und ein Interesse hieran auch für die Zukunft nicht erkannt wird. MW informiert die kommunalen Gewerbebehörden und die im Einzelfall fachlich berührten Institutionen, z. B. IHKn, regelmäßig über die Beratungen des Bund-/Länderausschusses „Gewerberecht“. Dies ist auch im vorliegenden Fall erfolgt.

Die betroffene Behörde wurde über die Sach- und Rechtslage informiert und hat ihre Vollzugspraxis angepasst.

Schule: Webbasierte Lernplattformen und Whiteboards

(TB, Seiten 40 bis 41)

Der Tätigkeitsbericht befasst sich auch mit der webgestützten Wissensvermittlung und der elektronischen Kommunikation zwischen Schülerinnen und Schülern und den Lehrkräften. Um auch hier datenschutzrechtliche Vorgaben einzuhalten, hatte die LfD dem Kultusministerium (MK) empfohlen, für die Nutzung von Lernplattformen Rahmenbedingungen festzulegen. Mit dem Einsatz digitaler Medien bedarf es weiter der Vermittlung eines Datenschutzbewusstseins der Lehrkräfte.

Die Entscheidung zum Einsatz von Lernplattformen trifft die eigenverantwortliche Schule. Bei der Entscheidungsfindung können Schulen auf die Unterstützung durch die medienpädagogische Beratung des Niedersächsischen Landesinstituts für schulische Qualitätsentwicklung (NLQ) vor Ort in den Medienzentren und auf das Informationsangebot auf dem niedersächsischen Bildungsserver (http://datenschutz.nibis.de) zurückgreifen. Die Sensibilisierung für Fragen des Datenschutzes ist Teil der Beratung.

Haben Schulen den Beschluss zur verbindlichen Einführung einer Kooperationsplattform gefasst, sind die davon betroffenen Nutzergruppen über den Umgang mit ihren personenbezogenen Daten zu informieren. Hierfür stehen Mustervorlagen zur Verfügung.

Unter http://datenschutz.nibis.de ist eine Rubrik „Kooperationsplattformen“ eingerichtet worden, die den Schulen umfassendes Informationsmaterial bis hin zu Mustervorlagen erforderlicher Dokumente bereitstellt. Darüber hinaus vertritt das MK die Ansicht, dass es Aufgabe der Anbieter ist, den Schulen entsprechende Dokumente gemäß den Vorschriften des NDSG zur Verfügung zu stellen. Den Schulen wird empfohlen, bei der Entscheidung für einen Anbieter gezielt nach diesen Dokumenten zu fragen.

Für die Unterstützung der behördlichen Datenschutzbeauftragten hat das NLQ gemeinsam mit der LfD ein Fortbildungskonzept erarbeitet, das durch ein Multiplikatorensystem regional umgesetzt wird. Die medienpädagogische Beratung bietet regelmäßig in ihren sechs Regionen entsprechende Veranstaltungen an. In einem gemeinsamen Arbeitskreis mit der LfD wird das Angebot laufend weiterentwickelt.

In den Bestimmungen für Lehramtsstudiengänge, den Vorbereitungsdienst und die Fort- und Weiterbildung der Lehrkräfte sind darüber hinaus keine weiteren Regelungen getroffen worden.

Die Regeln für den Einsatz privater IT-Systeme ergeben sich aus dem Runderlass „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Lehrkräften“ vom 01.02.2012. Zu dem Erlass finden sich weitergehende Informationen unter http://datenschutz.nibis.de im Informationsportal.

Einsatz von Microsoft Office 365 in Schulen

(TB, Seiten 42 bis 43)

Die LfD erachtet die Nutzung des Cloud-basierten Büropaketes Office 365 des Unternehmens Microsoft durch öffentliche Stellen wie Schulen als unzulässig. Die Datenverarbeitung in Form des Cloud Computing finde grundsätzlich in Form der Auftragsdatenverarbeitung statt. Eine solche Datenverarbeitung, bei der die Auftraggeber - hier die Schulen - weisungsbefugt gegenüber dem Auftragnehmer - hier das Unternehmen Microsoft - ist, sei in dieser Konstellation nicht denkbar. Im Übrigen sei nicht zweifelsfrei geklärt, ob die Daten nicht in außereuropäisches Ausland mit einem unzureichenden Datenschutz transferiert würden.

Im Informationsportal unter http://datenschutz.nibis.de ist im September 2013 ein kritischer Artikel zu Office 365 eingestellt worden. Darüber hinaus ist ein Beitrag der LfD zu Cloud-Angeboten US-amerikanischer Anbieter (hier: Google) eingestellt worden. Aus beiden Texten geht deutlich hervor, dass Schulen von einer Nutzung solcher Online-Dienste Abstand nehmen sollten. Die betreffende Passage aus dem vorliegenden Tätigkeitsbericht soll hier ebenfalls als Beitrag veröffentlicht werden.

Bei der Nutzung der Offline-Variante des Angebots Office 365 handelt es sich aber um einen anders zu bewertenden Sachverhalt: Da die Software lokal installiert wird und keine Online-Anbindung in der Nutzung erforderlich ist, erscheint dieses Angebot unverdächtig. Einzig bei der Registrierung der individuellen Lizenz könnte ein datenschutzrechtliches Problem auftreten, für dessen Lösung jedoch die anbietenden Unternehmen (in Deutschland: Fa. Cotec GmbH) eine nach eigener Auskunft datenschutzrechtlich einwandfreie Vorgehensweise entwickelt haben.

Datenschutz und Kindesunterhalt

(TB, Seite 47)

Der Tätigkeitsbericht befasst sich mit der Bemessung des Kindesunterhalts sowie der damit zusammenhängenden Datenübermittlung, die von der LfD in der geschilderten Fallsituation für zulässig erachtet wird.

Auch wenn hier keine Beanstandungen erfolgt sind, werden aus Sicht der Landesregierung zu der von der LfD dargestellten Rechtslage die folgenden Anmerkungen für erforderlich gehalten: Laut Bericht der LfD kennt das Gesetz keine festen Sätze, wie der angemessene Unterhalt auszufallen hat. Dies trifft nur grundsätzlich zu. Es sollte nicht unbeachtet bleiben, dass in § 1612 a des Bürger-

lichen Gesetzbuches (BGB) die Grundregeln für eine Bezifferung des Unterhalts festgelegt werden. Ergänzend ist zu bemerken, dass der Mindestunterhalt (der, falls der unterhaltspflichtige Elternteil unterhaltsrechtlich nicht leistungsfähig ist, durchaus unterschritten werden kann) nach aktuell geltendem Recht (nicht für den Berichtszeitraum) durch Verordnung vom 03.12.2015 (BGBl. I S. 2188) geregelt worden ist.

Weiter wird im Bericht ausgeführt: „Da der Kindesunterhalt in Natural- und Barunterhalt erbracht wird, wird davon ausgegangen, dass der Elternteil, bei dem das Kind lebt, den angemessenen Unterhalt in Form des Naturalunterhalts erbringt."

Diese Aussage ist rechtlich so nicht zutreffend. Das Verhältnis der elterlichen Unterhaltsverpflichtungen zueinander wird in § 1606 Abs. 3 BGB geregelt. Hier heißt es „Der Elternteil, der ein minderjähriges unverheiratetes Kind betreut, erfüllt seine Verpflichtung, zum Unterhalt des Kindes beizutragen, in der Regel durch die Pflege und die Erziehung des Kindes." Der Begriff Naturalunterhalt ist im Unterhaltsrecht hingegen nicht näher definiert.

Im Bericht wird weiter ausgeführt: „Die Unterhaltsbedarfssätze ergeben sich aus gerichtlichen Tabellen, in der Praxis werden häufig die Unterhaltssätze der sogenannten Düsseldorfer Tabelle angewandt."

Hierzu ist zu bemerken, dass sich die Höhe eines Unterhaltsanspruches nicht aus gerichtlichen Tabellen ergibt, sondern individuell berechnet wird. Die diversen gerichtlichen Tabellen können aufgrund der Vielschichtigkeit des Unterhaltsrechts lediglich als Leitlinien dienen. Von den meisten Gerichten wird die bundesweit fachlich anerkannte „Düsseldorfer Tabelle", die auch als Grundlage vieler anderer gerichtlicher Unterhaltstabellen dient, zur Orientierung herangezogen. Eine Verpflichtung der Gerichte, bei der Bemessung einer Barunterhaltsverpflichtung eine Unterhaltstabelle anzuwenden, besteht nicht.

Die Darstellung im Bericht über die Tätigkeit des Jugendamtes ist nicht zutreffend.

Bei der Führung einer Beistandschaft wird das Jugendamt nicht „im Sinne" des § 68 des Achten Sozialgesetzbuches (SGB VIII) tätig. Eine Beistandschaft ist ein privatrechtliches besonderes Schutzverhältnis, welches seine Grundlage in § 1712 BGB findet. Sie steht damit einer Pflegschaft oder Vormundschaft nahe. In § 2 Abs. 3 Nr. 11 SGB VIII wird klargestellt, dass diese dem Privatrecht zuzuordnende Aufgabe als andere Aufgabe der Kinder- und Jugendhilfe wahrgenommen wird.

Die §§ 55 und 56 SGB VIII geben den Rahmen der Beistandschaftsführung vor. Unter anderem wird festgestellt, dass die Person, die mit der Beistandschaftsführung beauftragt wird, gesetzliche Vertreterin bzw. gesetzlicher Vertreter des betroffenen Kindes bzw. Jugendlichen ist (§ 55 Abs. 3 Satz 2 SGB VIII). Im eigentlichen Sinn wird die Beistandschaft daher nicht vom Jugendamt, sondern von entsprechend beauftragten Beschäftigten eines Jugendamtes geführt. Diese sind als gesetzliche Vertreterin oder gesetzlicher Vertreter im Hinblick auf die konkrete Aufgabenwahrnehmung keinen dienstlichen Weisungen unterworfen.

§ 68 SGB VIII regelt die mit der Führung von Beistandschaften zusammenhängenden Fragen des Datenschutzes. Nach § 61 Abs. 2 SGB VIII gilt für die Führung der Beistandschaft nur § 68 SGB VIII. Die datenschutzrechtlichen Regelungen in § 68 SGB VIII sind damit abschließend. Diese grundsätzlichen Bemerkungen vorweggestellt, erscheinen noch folgende Einzelanmerkungen geboten:

– Nicht die Leistungsfähigkeit des unterhaltsverpflichteten Elternteils wird geprüft, sondern allenfalls dessen unterhaltsrechtliche Leistungsfähigkeit.

– Ein Beistand ist nicht verpflichtet, Nachweise über die wirtschaftlichen Verhältnisse eines Elternteils zu erheben. In Abstimmung mit dem die Beistandschaft beantragenden Elternteil kann eine Unterhaltsforderung beispielweise ohne Prüfung der wirtschaftlichen Verhältnisse auf einen Festbetrag begrenzt werden. Es könnte gleichfalls vereinbart werden, dass Angaben des unterhaltsverpflichteten Elternteils vertraut werden kann, ohne dass eine Vorlage von Unterlagen erforderlich ist.

– Selbstverständlich steht es allen Betroffenen frei, die von einem Beistand vorgenommene Unterhaltsberechnung zu überprüfen. Der Beistand wird seine Berechnung in der Regel auch allen Betroffenen gegenüber gerne erläutern. Eine Überprüfung der Berechnung im engeren Sinne bietet ein Beistand allerdings für keinen Elternteil an. Der Beistand ist Interessenvertreter des Kindes und nicht eines Elternteils.

– Unabhängig davon, welcher Elternteil barunterhaltspflichtig ist und welcher nicht, ist es nicht zwingend, in jedem Fall oder gar von beiden Elternteilen Daten über die wirtschaftlichen Verhältnisse zu erheben. Die wirtschaftlichen Verhältnisse des das Kind betreuenden Elternteils sind nur bedingt von Bedeutung, sofern eine über dem Mindestunterhalt liegende Unterhaltsforderung geltend gemacht wird und auch nur dann, wenn das Einkommen des das Kind betreuenden Elternteils das Einkommen des barunterhaltspflichtigen Elternteils deutlich übersteigt.

– Eine Weitergabe von Daten über die wirtschaftlichen Verhältnisse eines Elternteils an den anderen Elternteil stellt während des Zeitraums der Führung der Beistandschaft einen eindeutigen Verstoß gegen den Sozialdatenschutz dar. § 68 SGB VIII enthält keine entsprechende Ermächtigung zur Datenweitergabe. Lediglich nach Aufhebung der Beistandschaft hat der Elternteil, der ursprünglich die Einrichtung der Beistandschaft beantragt hat, (unter bestimmten Voraussetzungen) das Recht, Daten zu erhalten (§ 68 Abs. 3 Satz 3 SGB VIII).

– Ein gemeinsames Gespräch beim Jugendamt kann bei grundsätzlicher Gesprächsbereitschaft beider Elternteile stets eine gute Grundlage für die weitere Zusammenarbeit im Interesse eines gemeinsamen Kindes sein. Die Erhebung einer Beschwerde bei der Datenschutzbeauftragten dürfte andererseits das Wohl eines Kindes nicht berühren.

Behördliche Datenschutzbeauftragte

(TB, Seite 56)

In ihrem Bericht bemängelt die LfD, dass viele Schulen noch keine behördlichen Datenschutzbeauftragten bestellt hätten.

MK sieht das Erfordernis, dass die Schulen in Niedersachsen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten nach § 8 a NDSG zu bestellen haben. Insbesondere auch aufgrund der Vielzahl von kleinen Schulen und der Komplexität des Themas Datenschutz ist die Bestellung von Datenschutzbeauftragten in jeder Schule noch nicht flächendeckend erfolgt. In Kenntnis der Problematik hat MK ein Konzept erstellt, welches es den Schulen erleichtern soll, Datenschutzbeauftragte zu bestellen.

Das Konzept sieht vor, in der Niedersächsischen Landesschulbehörde langfristig jeweils zwei „Beauftragte für Datenschutzangelegenheiten der Schulen“ pro Regionalabteilung zu etablieren, die sowohl über datenschutzrechtliche Kenntnisse als auch Informatikkenntnisse verfügen. Die ersten beiden Stellen werden im ersten Quartal 2016 besetzt werden. Zu den Aufgaben dieser Beauftragten gehört dann vornehmlich die Beratung der Datenschutzbeauftragten der Schulen vor Ort. Daneben soll aber auch die Möglichkeit bestehen, dass die Beauftragten von einzelnen Schulen als Datenschutzbeauftragte gemäß § 8 a NDSG bestellt werden können.

In einem ersten Schritt wird sich die Niedersächsische Landesschulbehörde einen Überblick verschaffen, wie viele Schulen in Niedersachsen bereits über Datenschutzbeauftragte verfügen und welcher Beratungsbedarf an den Schulen besteht. Nach Auswertung der Bestandsaufnahme und der gesammelten Erfahrungen soll in einem zweiten Schritt eine Beratung der Schulen zur Bestellung von Datenschutzbeauftragten erfolgen und die weitere Umsetzung des Konzeptes in Angriff genommen werden. Langfristig wird die Umsetzung des Konzeptes dazu führen, dass die Schulen ihrer rechtlichen Verpflichtung, Datenschutzbeauftragte nach § 8 a NDSG zu bestellen, nachkommen.

Betriebliche Datenschutzbeauftragte

(TB, Seiten 58 bis 59)

Der Tätigkeitsbericht geht auch auf die zu erwartenden Änderungen durch die Datenschutz-Grundverordnung bei der Benennung von behördlichen und betrieblichen Datenschutzbeauftragten

ein. Die vorläufige Fassung des Einigungstextes sieht eine Verpflichtung zur Benennung einer oder eines Datenschutzbeauftragten vor für Behörden und öffentliche Stellen sowie für alle weiteren (privaten) Stellen, deren Kerntätigkeit im Hinblick auf die Verarbeitung personenbezogener Daten eine Benennung erforderlich macht. Dabei kommt es darauf an, welche und in welchem Umfang Daten verarbeitet werden. Den Mitgliedstaaten wird darüber hinaus die Möglichkeit eröffnet, weitere Gruppen datenverarbeitender Stellen zur Benennung von Datenschutzbeauftragten zu verpflichten. Die freiwillige Benennung soll den verantwortlichen Stellen in jedem Fall möglich sein.

Beschäftigtendatenschutz

(TB, Seiten 86 bis 87)

Wie bereits im vorangegangenen Berichtszeitraum wird die Bedeutung umfassender klarer Regelungen zum Beschäftigtendatenschutz zumindest auf dem Niveau derzeitiger deutscher Datenschutzstandards betont.

Die Landesregierung unterstreicht diese Bedeutung. Die Datenschutz-Grundverordnung wird die Mitgliedstaaten zum Erlass spezifischer Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten bei der Datenverarbeitung im Beschäftigtenkontext ermächtigen, sodass in diesem Bereich detaillierte Regelungen geschaffen werden können. Dabei wird der Diskussionsprozess aus der Vergangenheit mit den unterschiedlichen Interessen und Erwartungen der Beschäftigten, der Arbeitgeberinnen und Arbeitgeber sowie der Interessenvertretungen fortzuführen sein.

Kameras in Bussen und Bahnen

(TB, Seiten 92 bis 95)

Die LfD bemängelt in ihrem Bericht, dass eine Einzelfallprüfung vor dem Einsatz von Anlagen zur Videoüberwachung (VÜ) in der Praxis nicht mehr stattfinde und die VÜ überwiegend allgemein mit dem Sicherheitsbedürfnis der Fahrgäste begründet werde. Zudem könne das Sicherheitsbedürfnis nur ausreichend über ein Monitoringverfahren mit Liveübertragung der Bilder befriedigt werden, bei denen eine unmittelbare Reaktion erfolgen kann. Die praktizierte Aufzeichnung der Bilder (sogenanntes Black-Box-Verfahren) und spätere Auswertung nur bei Bedarf könne dies nicht erfüllen.

Die Aufgabenträger des Öffentlichen Personennahverkehrs (ÖPNV) in Niedersachsen und hier vornehmlich die drei niedersächsischen Aufgabenträger des Schienenpersonennahverkehrs (SPNV) - so auch die Landesnahverkehrsgesellschaft Niedersachsen (LNVG) - befürworten die Videoüberwachung mittels des Black-Box-Verfahrens und sehen in deren Einsatz neben der Bemessung einer ausreichenden Anzahl von Zugbegleiterinnen und Zugbegleitern und besonders geschultem zusätzlichen Sicherheitspersonal einen wesentlichen Baustein eines umfassenden Sicherheitskonzepts. Dementsprechend sind oder werden auch die neueren zum Einsatz kommenden SPNV-Fahrzeuge der LNVG und auch der beauftragten Eisenbahnverkehrsunternehmen überwiegend mit Videokameras ausgestattet. Durch den Einsatz der videoüberwachten Fahrzeuge soll die politisch erwünschte verstärkte Nachfrage im ÖPNV und insbesondere im SPNV weiter gefördert und vor allem die Vorteile des umweltschonenden und technisch gegenüber anderen Verkehrsträgern besonders sicheren SPNV genutzt werden, um den Modal Split (Aufteilung der Verkehrsteilnehmer auf Verkehrsträger) für diesen Verkehrsträger für die Zukunft weiter zu verbessern. In diesem Kontext kommt dem subjektiven Sicherheitsgefühl der Fahrgäste und auch dem des Personals der Verkehrsunternehmen eine besondere Bedeutung zu.

Für die Videoüberwachung mittels Black-Box-Verfahren besteht entgegen der Ansicht der LfD ein berechtigtes Interesse im Sinne des § 6 b BDSG. Wenn dazu in dem Bericht der LfD auf Seite 93 ausgeführt wird, dass für die Annahme eines berechtigten Interesses im Sinne der vorgenannten Vorschrift konkrete Tatsachen in der Vergangenheit zu fordern sind, aus denen sich eine konkrete Gefährdung für die Zukunft ergebe, so ist dem entgegenzuhalten, dass Vorkommnisse in der Vergangenheit zwar eine Gefährdungslage für die Zukunft indizieren können, jedoch andererseits das Fehlen des Nachweises solcher Vorkommnisse gerade kein Beweis dafür ist, dass nicht von einer Gefährdung ausgegangen werden kann. In diesem Zusammenhang ist beispielhaft auf die überregional bekannt gewordenen Fälle in München hinzuweisen, die sich gerade an Bahnhöfen ereignet haben, an denen in der Vergangenheit keine besonderen Auffälligkeiten bestanden und die bisher auch nicht als Kriminalitätsschwerpunkte aufgefallen waren. Folgerichtig hat auch das Oberverwal-

tungsgericht Lüneburg in seiner Entscheidung vom 29.09.2014, 11 LC 114/13, im Falle eines videoüberwachten öffentlich zugänglichen Teils eines Bürogebäudes ausgeführt, dass der Einsatz von Videotechnik zum Zwecke der Gefahrenabwehr sowohl unter dem Gesichtspunkt des Hausrechts als auch zur Wahrnehmung berechtigter Interessen erfolgen darf.

Ob und in welchem Umfang eine Übertragbarkeit dieser Grundsätze auf den ÖPNV und SPNV erfolgen kann, werden die Entscheidungen in weiteren Verfahren ergeben.

Die Veröffentlichung von Videobildern durch die Polizei trägt wesentlich zur Täteridentifizierung und Täterergreifung bei und hat in vielen Fällen sogar dazu geführt, dass sich Täterinnen oder Täter sehr zeitnah nach Veröffentlichung von Bildern selbst der Polizei gestellt haben. In diesem Zusammenhang ist ergänzend zu berücksichtigen, dass einerseits an den eingesetzten Fahrzeugen selbst deutlich erkennbare Hinweise auf die Videoüberwachung angebracht sind und andererseits der Hinweis auf die mögliche Videoüberwachung im Fahrzeug auch Bestandteil der Beförderungsbedingungen im Niedersachsentarif und damit auch Bestandteil des jeweiligen Beförderungsvertrages ist.

Gleiches gilt für die eingesetzte Videoüberwachung an Bahnhöfen im Eigentum der Eisenbahnen des Bundes. Gerade aktuellen Presseberichten der letzten Zeit ist zu entnehmen, dass die Anzahl der Straftaten in oder im Umfeld von Bahnhöfen im letzten Jahr stark zugenommen hat und deshalb die Videoüberwachung in diesen ebenfalls hochfrequentierten Anlagen eher verstärkt von der hier nach § 3 Bundespolizeigesetz (BPolG) zuständigen Bundespolizei unter Anwendung des § 27 BPolG zur Gefahrenabwehr und Täterermittlung eingesetzt werden soll. Dass an Bahnhöfen das Mittel der Videoüberwachung ebenfalls im Black-Box- und nicht im Monitoringverfahren auf der Grundlage der vorgenannten gesetzlichen Regelung zur Gefahrenabwehr eingesetzt werden darf, ist von der insoweit zuständigen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bisher nie in Zweifel gezogen worden. Die unterschiedliche Behandlung von Bahnhöfen im Eigentum der Eisenbahnen des Bundes einerseits (§ 27 BPolG) sowie Bahnhöfen anderer Eigentümer und Nahverkehrsfahrzeugen andererseits in Bezug auf die Zulässigkeit von Videoüberwachung erscheint vor dem Hintergrund eines Gesamtangebotes für die Fahrgäste nicht nachvollziehbar. Am 15.04.2016 hat deshalb auch die Verkehrsministerkonferenz auf Initiative Niedersachsens durch einstimmigen Beschluss dafür votiert, die Innenministerkonferenz darum zu bitten, im Sinne einer einheitlichen Sicherheitsphilosophie im öffentlichen Personenverkehr darauf hinzuwirken, die geltenden datenschutzrechtlichen Vorgaben entsprechend den Regelungen im Bundespolizeigesetz anzupassen.

Anders als in dem Bericht der LfD auf Seite 92 ausgeführt, verstößt der Einsatz von Videokameras im Black-Box-Verfahren auch nicht gegen das Gebot der Datenvermeidung und der Datensparsamkeit des § 3 a BDSG.

§ 3 a BDSG fordert eine Ausrichtung an dem Ziel, „so wenig personenbezogene Daten wie möglich“ zu erheben. Diese Vorgabe wird aber durch den Einsatz der Videokameras im Black-Box-Verfahren eingehalten. In diesem Verfahren werden Videoaufnahmen ohne Ton lediglich für eine Zeit zwischen 24 und maximal 72 Stunden aufgezeichnet und ohne Auslesen automatisch wieder überschrieben, es sei denn, dass sich Straftaten ereignen und die Bilder unter Beteiligung der zuständigen Polizeidienststellen zur Täterermittlung ausgelesen werden. Insofern wird Videoaufzeichnung auf das erforderliche Mindestmaß begrenzt.

Eine weitere Verringerung der Aufzeichnung ist nicht möglich. Würden nämlich - wie dies die LfD auf Seite 93 ihres Berichts fordert - außer den zum geschützten Intimbereich gehörenden Toiletten weitere videofreie Räume als sogenannte „Privatzonen“ im Fahrzeug eingerichtet und auch entsprechend gekennzeichnet, wären die mit dem Videoeinsatz verbundenen Ziele der subjektiven Sicherheit für die Fahrgäste, der Prävention sowie auch der Schutz vor Straftaten sowie das repressive Ziel der Täterermittlung in diesem Bereich aufgehoben.

Soweit die LfD in ihrem Bericht auf Seite 94 ausführt, dass die Videoüberwachung im Fahrzeug zu rein präventiven Zwecken eingesetzt werde und deshalb nicht erforderlich im Sinne des § 6 b BDSG sei, weil eine Beobachtung des Geschehens über Monitore (Monitoring-Modus) als ein in das Persönlichkeitsrecht der Fahrgäste weniger einschneidende Mittel mit gleichem Erfolg eingesetzt werden könne, so kann diesen Ausführungen im Ergebnis aus mehreren Gründen nicht zuge-

stimmt werden. Zum einen ist die dauerhafte Überwachung über Monitore im Vergleich zum Black-Box-Verfahren, in dem die Videoaufnahmen nur dann ausgelesen werden, soweit besondere Ereignisse mit strafrechtlicher Relevanz vorfallen, nicht das mildere, sondern im Gegenteil gegenüber den Fahrgästen und dem Personal das stärker eingreifende Mittel.

So hat auch das OVG Lüneburg in seiner bereits zitierten Entscheidung dazu richtigerweise ausgeführt, dass auch der Einsatz von Wachpersonal anstelle von Videoüberwachung im Black-Box-Verfahren schon deshalb nicht in Betracht kommen könne, weil eine permanente Überwachung durch Personal gegenüber einer Videoüberwachung im Black-Box-Verfahren sich als subjektiv gravierenderer Eingriff darstelle. Dies führt das Gericht entsprechend auch für die Überwachung im Monitoring-Modus aus. Im Übrigen hat das OVG Lüneburg zu Recht darauf hingewiesen, dass zusätzliches Personal zur dauerhaften Überwachung kaum in gleicher Weise geeignet sein kann, den gewünschten Zweck zu erreichen, da das eingesetzte Personal nicht zu jeder Zeit an allen überwachten Orten zugleich sein könnte. Darüber hinaus seien auch die Kosten für den Einsatz von zusätzlichem Personal gegenüber dem Betrieb einer Videoanlage ungleich höher und damit wirtschaftlich nicht vertretbar.

Insoweit ist festzustellen, dass das Monitoringverfahren kein Ersatz für das bisher praktizierte Videoüberwachungsverfahren sein kann und damit die Erforderlichkeit im Sinne des § 6 b BDSG entgegen der Auffassung der LfD gegeben ist.

Letztlich spricht auch bei einer sachgerechten Interessenabwägung in Bezug auf die Fahrgäste im ÖPNV nichts gegen den bisher praktizierten Einsatz der Videoüberwachung. So ist bei der LNVG und, soweit ersichtlich, auch bei anderen SPNV-Aufgabenträgern in Niedersachsen trotz der Vielzahl der eingehenden Kundenbeschwerden im ÖPNV keine einzige Kundenbeschwerde über den Einsatz von Videokameras in Fahrzeugen bekannt. Daraus wird sehr deutlich erkennbar, dass, anders als in dem Bericht der LfD auf Seite 94 dargestellt, die Fahrgäste nicht von der Videoüberwachung verschont werden wollen, sondern dass die Mitarbeiterinnen und Mitarbeiter und auch die Fahrgäste des jeweiligen Verkehrsunternehmens, wie entsprechende Kundenumfragen belegen, ganz im Gegenteil ein sehr hohes Interesse an der eigenen Sicherheit im Fahrzeug haben und den Einsatz von Videoaufnahmen zu ihrer eigenen Sicherheit ausdrücklich begrüßen, vereinzelt sogar einfordern, wie z. B. der Seniorenbeirat der Landeshauptstadt Hannover.

Leider ist aus dem vorgelegten Bericht der LfD nicht erkennbar, ob und inwieweit sich die LfD mit der gebotenen Güterabwägung zwischen dem Recht auf informationelle Selbstbestimmung des einzelnen Fahrgastes und dem erkennbaren Willen und Interesse der weit überwiegenden Anzahl der Fahrgäste an der praktizierten Videoüberwachung auseinandergesetzt hat.

Abschließend ist anzumerken, dass der Klärung der Frage der Rechtmäßigkeit der nicht nur in Niedersachsen, sondern bundesweit im ÖPNV und hier vornehmlich im SPNV praktizierten Videoüberwachung gerade vor dem Hintergrund der zunehmenden Straftaten im ÖPNV eine besondere Bedeutung zukommt. Dies gilt umso mehr, weil einerseits der Düsseldorfer Kreis und somit insbesondere auch die LfD nach der Verabschiedung der Orientierungshilfe davon ausgehen, dass alle Aufgabenträger diese Orientierungshilfe als rechtlich bindend für künftige Ausschreibungen ansehen und andererseits bisher zu der hier strittigen Frage der rechtlichen Zulässigkeit der praktizierten Videoüberwachung soweit ersichtlich bundesweit noch keine Gerichtsentscheidung vorliegt, die die Rechtsauffassung der Datenschutzbehörden bestätigt.

In diesem Zusammenhang ist darauf hinzuweisen, dass die LfD bereits durch Verfügung vom 29.10.2014, also lange vor der Verabschiedung der Orientierungshilfe am 16.09.2015, der üstra aufgegeben hat, die in ihren Fahrzeugen installierten und im Black-Box-Verfahren eingesetzten Videokameras zum 01.10.2014 unter Hinweis auf die angebliche datenschutzrechtliche Unzulässigkeit abzustellen. Gegen diesen auch bundesweit bekanntgewordenen und viel diskutierten Bescheid hat die üstra am 30.09.2014 Anfechtungsklage vor dem Verwaltungsgericht Hannover erhoben, der am 10.02.2016 - allerdings aus rein formellen Gründen - stattgegeben wurde. Wegen der grundsätzlichen Bedeutung wurde die Berufung zum Niedersächsischen Oberverwaltungsgericht zugelassen. Die LfD hat inzwischen die Berufung eingelegt.

Videoüberwachung an Schulen

(TB, Seite 107)

Die LfD erläutert in ihrem Bericht die Voraussetzungen für eine zulässige Videoüberwachung an Schulen.

Die Auffassung der LfD zu dieser Thematik wird geteilt. Die Schulen in Niedersachsen werden bereits entsprechend beraten. Auf der Homepage des NLQ zum Thema Datenschutz wird hierzu § 25 a NDSG aufgeführt und näher erläutert. Eine Videoüberwachung an Schulen ist danach grundsätzlich unzulässig. Gewalttätigen Konflikten, Vandalismus u. ä. ist mit anderen - pädagogischen - Mitteln zu begegnen. Nur in Fällen, in denen alle anderen Maßnahmen nicht zum Erfolg führen, kann ausnahmsweise die Videoüberwachung bestimmter Räumlichkeiten für einen begrenzten Zeitraum angezeigt sein. Die flächendeckende Überwachung von Eingangsbereichen, Fluren und Unterrichtsräumen ist hingegen generell unzulässig.

Wenn beispielsweise das Schulgebäude immer wieder durch Vandalismus beschädigt oder durch Graffiti beschmiert wird und andere Maßnahmen (verstärkte Streifentätigkeit der Polizei, Kontrollen durch den Hausmeister etc.) erfolglos geblieben sind, kann es zulässig sein, eine Videoüberwachung einzusetzen. Dabei muss aber i. d. R. sichergestellt sein, dass die Videoüberwachung nur außerhalb des Schulbetriebes erfolgt.

Videoüberwachte Gerichtsgebäude

(TB, Seiten 108 bis 109)

Im Rahmen einer Schwerpunktprüfung hat die LfD im Berichtszeitraum die Videoüberwachung in und an Gerichtsgebäuden geprüft. Dabei festgestellte Mängel und Beanstandungen wurden im Anschluss zusammen mit den verantwortlichen Stellen ausgeräumt.

Die Landesregierung betont in Übereinstimmung mit der LfD die Notwendigkeit, die Videoüberwachung auf das unabwendbar notwendige Maß zu beschränken. Das Justizministerium (MJ) hatte in diesem Zusammenhang bereits Ende 2014 die Gerichte und Staatsanwaltschaften auf die besondere Bedeutung von Vorabkontrollen und Verfahrensbeschreibungen im Zusammenhang mit Videoüberwachungsanlagen hingewiesen. Auch wurden die Behörden gebeten, die Erstellung der Verfahrensbeschreibungen nachzuholen, falls dies bisher unterblieben ist. Im Rahmen der Umsetzung des Sicherheitskonzeptes 2014 beabsichtigt das MJ, die Frage der Videoüberwachung mit den Gerichten und Staatsanwaltschaften zu erörtern und - sofern erforderlich und möglich - Kriterien für die Erforderlichkeit und inhaltliche Ausgestaltung von Videoüberwachungen zu erarbeiten.

Der Bericht der LfD wurde zum Anlass genommen, die Gerichte und Staatsanwaltschaften erneut für den Datenschutz bei Videoüberwachung zu sensibilisieren und auf die Kennzeichnung hinzuwirken.

Europa und internationaler Datenverkehr

Europäische Datenschutzreform

(TB, Seiten 110 bis 112)

Anknüpfend an den letzten Tätigkeitsbericht stellt die LfD den Sachstand 2014 zur europäischen Datenschutzreform dar und benennt aus Sicht der Aufsichtsbehörden wesentliche Punkte, die bei der Reform berücksichtigt werden sollten.

Inzwischen wurden die Verhandlungen auf europäischer Ebene zwischen der Kommission (KOM), dem Rat und dem Parlament sowohl zur Datenschutz-Grundverordnung als auch zur Richtlinie für die Polizei und den Justizbereich abgeschlossen, das Ergebnis liegt aktuell in einer vorläufigen Fassung vor. Sobald der Einigungstext in den Sprachfassungen der Mitgliedstaaten vorliegt, soll die formelle Annahme der Fassung von den europäischen Gremien erfolgen. Die Datenschutz-Grundverordnung wird voraussichtlich Mitte des Jahres 2016 in Kraft treten und zwei Jahre später von den Mitgliedstaaten anzuwenden sein. Die Datenschutzressorts des Bundes und der Länder bereiten bereits intensiv den Umsetzungsprozess vor.

Die Datenschutz-Grundverordnung wird unmittelbar in den Mitgliedstaaten gelten und anzuwenden sein, in einzelnen Bereichen werden die Mitgliedstaaten ermächtigt, spezifischere Regelungen zu erlassen. Die Verordnung wird auch für öffentliche Stellen gelten und von diesen anzuwenden sein. Die Aufsichtsbehörden für den Datenschutz erhalten weitgehende Befugnisse, auch gegenüber öffentlichen Stellen.

Nach dem sogenannten „One-stop-shop"-Prinzip haben die Bürgerinnen und Bürger das Recht, sich im Falle einer Beschwerde in der gesamten EU nur noch an die Datenschutzbehörde ihres Mitgliedstaates zu wenden, gleich, wo der mögliche Datenschutzverstoß sich ereignet hat. Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten müssen bei grenzüberschreitender Datenverarbeitung nur noch mit der Datenschutzbehörde des Mitgliedstaates zusammenarbeiten, in dem sich der Hauptsitz des Unternehmens befindet. Die Rechte der Bürgerinnen und Bürger werden im Hinblick auf die Verarbeitung ihrer persönlichen Daten gestärkt. So wird u. a. ein Recht der Betroffenen auf Löschung ihrer Daten geschaffen, wonach die Daten verarbeitende Stelle die Daten nicht nur bei sich selbst zu löschen hat. Vielmehr hat die Stelle die Löschanfrage auch an Dritte, die die Daten verarbeiten, weiterzuleiten, die dann ebenfalls die Daten einschließlich aller Links hierzu zu löschen haben. Die Verordnung schafft ein Recht auf Datenportabilität, das den Betroffenen die Möglichkeit gibt, bei einem Anbieterwechsel ihre Daten in einem allgemein nutzbaren Format mitzunehmen. Daten verarbeitende Stellen müssen ihre Dienste möglichst datensparsam konzipieren und datenschutzfreundliche Voreinstellungen vornehmen. Auf weitere Regelungen der Datenschutz-Grundverordnung wird zu einzelnen Themen in dieser Stellungnahme eingegangen.

Internationaler Datenverkehr und Geheimdiensttätigkeit - Safe Harbor

(TB, Seiten 113 bis 115)

Im Abschnitt „internationaler Datenverkehr" kritisiert die LfD auf dem Sachstand von 2013 Datenübermittlungen in die USA auf der Basis des Safe-Harbor-Abkommens. In dem Abkommen zwischen der EU und den USA aus dem Juli 2000 wurden Vereinbarungen getroffen, nach denen bei den Unternehmen, die dem System Safe Harbor beigetreten sind, ein angemessener Schutz für die EU-Bürgerinnen und -Bürger beim Umgang mit ihren personenbezogenen Daten in den USA gewährleistet wird.

Aus Sicht der Datenschutzbeauftragten des Bundes und der Länder griff das Abkommen bzw. das Verfahren zu kurz. Daten exportierende Unternehmen dürften sich nicht auf die Erklärung von US-Unternehmen verlassen, dem Abkommen beigetreten zu sein bzw. sich zertifiziert zu haben. Die Unternehmen müssten dies vielmehr nachweisen, was auch nachgeprüft werden müsste. Die KOM stand seit dem Jahr 2013 in Verhandlungen mit den USA über Nachbesserungen zu dem Abkommen.

Inzwischen hat der Europäische Gerichtshof (EuGH) mit Urteil vom 06.10.2015 in der Rechtssache C-362/14 festgestellt, dass die Existenz einer Entscheidung der KOM, in der festgestellt wird, dass ein Drittland ein angemessenes Schutzniveau für übermittelte personenbezogene Daten gewährleistet, die Befugnisse, über die die nationalen Datenschutzbehörden aufgrund der Charta der Grundrechte der Europäischen Union und der Richtlinie verfügen, weder beseitigen noch auch nur beschränken kann. Auch wenn die KOM eine solche Entscheidung erlassen hat, müssen die nationalen Datenschutzbehörden in völliger Unabhängigkeit prüfen können, ob bei der Übermittlung der Daten einer Person in ein Drittland die in der Richtlinie aufgestellten Anforderungen gewahrt werden.

Der EuGH führt weiter aus, dass das Safe-Harbor-Abkommen nur für die amerikanischen Unternehmen gilt, die sich ihm unterwerfen, nicht aber für die Behörden der USA. Außerdem haben die Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses und der Durchführung von Gesetzen der USA Vorrang vor der Safe-Harbor-Regelung, sodass die amerikanischen Unternehmen ohne jede Einschränkung verpflichtet sind, die in dieser Regelung vorgesehenen Schutzregeln außer Acht zu lassen, wenn sie in Widerstreit zu solchen Erfordernissen stehen.

Zum Vorliegen eines Schutzniveaus, das den in der EU garantierten Freiheiten und Grundrechten der Sache nach gleichwertig ist, muss eine Regelung die Datenspeicherung auf das absolut Notwendige beschränken. Dies ist nicht der Fall, wenn sie generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der EU in die USA übermittelt werden, ge-

stattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne objektive Kriterien vorzusehen, die es ermöglichen, den Zugang der Behörden zu den Daten und deren spätere Nutzung zu beschränken. Darüber hinaus besteht keine Möglichkeit für die Bürgerinnen und Bürger, mittels eines Rechtsbehelfs Zugang zu den sie betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken.

Aus diesen Gründen hat der Gerichtshof die Entscheidung der KOM zum Abkommen für ungültig erklärt. Das Urteil hat zur Folge, dass auch für den Datentransfer in die USA derzeit nur die Datenschutz-Richtlinie von 1995 gilt und auf dieser Grundlage Standardvertragsklauseln und verbindliche Unternehmensrichtlinien (Binding Corporate Rules) abgeschlossen werden können.

Die EU und die USA haben sich im Februar 2016 auf den Entwurf eines Nachfolgeabkommens geeinigt (Privacy Shield). Der Entwurf soll nach Anhörung und Stellungnahme der hierfür zuständigen Gremien durch einen Angemessenheitsbeschluss der KOM zur Grundlage für künftige Datenübermittlungen in die USA werden.

Die Art.-29-Gruppe - das Datenschutzteam für Europa

(TB, Seite 116)

Eine weitere wesentliche Änderung durch die Datenschutzreform der EU wird sich bei der Zusammenarbeit der Aufsichtsbehörden auf europäischer Ebene ergeben. Das von der LfD in ihrem Bericht beschriebene derzeitige Gremium gemäß Artikel 29 der Datenschutzrichtlinie der EU von 1995 mit allgemein beratender Funktion zu Fragen des Datenschutzes wird künftig durch den Europäischen Datenschutzausschuss abgelöst. Der Ausschuss soll die einheitliche Anwendung des Datenschutzrechts sicherstellen. In Fällen, in denen mehrere Mitgliedstaaten betroffen sind, kann er rechtlich verbindliche Entscheidungen treffen.

Fluggastdaten

(TB, Seiten 117 bis 118)

Der Tätigkeitsbericht informiert über den Verlauf der Beratungen auf europäischer Ebene über eine allgemeine Richtlinie zur Speicherung von Fluggastdaten. Nachdem ein Vorschlag der KOM vom Europäischen Parlament im Jahr 2013 zunächst abgelehnt worden war, wurden die Beratungen im Jahr 2015 wieder aufgenommen. Der Rat der Europäischen Union hat am 04.12.2015 die zuvor mit dem Europäischen Parlament ausgehandelte Kompromissfassung einer Richtlinie über die Verwendung von Fluggastdatensätzen (Passenger Name Records - PNR) zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität gebilligt. Die Fassung enthält u. a. Bestimmungen über den Austausch von PNR-Daten zwischen den Mitgliedstaaten und zwischen den Mitgliedstaaten und Drittstaaten. Die Passagierdaten sollen sechs Monate gespeichert werden; danach werden sie unkenntlich gemacht und für weitere viereinhalb Jahre gespeichert werden, in denen der Zugriff auf die vollständigen Daten strengen Regeln unterliegt.

Die Richtlinie wurde im April 2016 vom Europäischen Parlament verabschiedet. Die Mitgliedstaaten haben nun die Rechtsvorschriften zu erlassen, die erforderlich sind, um der Richtlinie nachzukommen.

Facebook

(TB, Seiten 131 bis 135)

Die LfD beanstandet in ihrem Tätigkeitsbericht den Einsatz von Facebook-Fanpages aus datenschutzrechtlichen und technisch-organisatorischen Gründen.

Der Landesregierung ist bewusst, dass das Unternehmen Facebook einen problematischen Umgang mit personenbezogenen Daten pflegt. Vor diesem Hintergrund hat die Landesregierung intensiv abgewogen, ob und in welcher Weise Facebook für die direkte Kommunikation mit Bürgerinnen und Bürgern genutzt werden soll. Letztlich haben die große Zahl von Facebook-Nutzerinnen und -Nutzern - insgesamt sind es rund 28 Millionen in Deutschland - und der Wunsch, die Bürgerinnen und Bürger nicht nur über die herkömmlichen Medien, sondern direkt über die Aktivitäten der Landesregierung informieren zu können, den Ausschlag gegeben. Soziale Netzwerke und insbesonde-

re Facebook bieten der Landesregierung auch die Möglichkeit, mit Bürgerinnen und Bürgern in einen Dialog zu treten. Die Presse- und Informationsstelle der Landesregierung fühlt sich ihrer Informationspflicht für alle Teile der Gesellschaft verpflichtet und bietet daher als zusätzliches Angebot eine Facebook-Seite an. Die Pressestelle der Landesregierung hat die LfD stets über ihre Facebook-Aktivitäten informiert. Daneben wird im Geschäftsbereich des Ministeriums für Wissenschaft und Kultur, des Ministeriums für Soziales, Gesundheit und Gleichstellung sowie im Ministerium für Wirtschaft, Arbeit und Verkehr in eigener Zuständigkeit durch die jeweilige Pressestelle eine Facebook-Seite für die Ministerin bzw. den Minister betrieben.

Zuständig für die Beurteilung der Zulässigkeit der Datenverarbeitung in Deutschland und für die Kontrolle über die Einhaltung der datenschutzrechtlichen Vorschriften sind gemäß § 1 Abs. 5 Satz 5 und § 38 Abs. 1 Satz 1 BDSG die deutschen Aufsichtsbehörden, d. h. die Beauftragten für den Datenschutz der Länder (siehe dazu und zu Folgendem auch die Antwort der Landesregierung vom 21.05.2015 auf die schriftliche Anfrage „Neue Datenrichtlinien von Facebook“ in der Drucksache 17/3573).

Die Zulässigkeit der Verarbeitung personenbezogener Daten bemisst sich für nicht öffentliche Stellen wie das Unternehmen Facebook grundsätzlich nach dem BDSG. § 1 Abs. 5 BDSG bestimmt dabei das anzuwendende Recht für die Fälle, in denen die für die Datenverarbeitung verantwortliche Stelle keinen maßgeblichen Sitz in der Bundesrepublik Deutschland hat. Soweit die Datenverarbeitung durch eine verantwortliche Stelle mit Sitz in einem anderen Mitgliedstaat der Europäischen Union erfolgt, findet das BDSG gemäß § 1 Abs. 5 Satz 1 keine Anwendung. Nach derzeit herrschender Rechtsauffassung deutscher Gerichte ist bei der Beurteilung der Zulässigkeit der Datenverarbeitung durch Facebook irisches Recht zugrunde zu legen.

Nach Auffassung des Schleswig-Holsteinischen Oberverwaltungsgerichts (siehe das allerdings noch nicht rechtskräftige Urteil vom 5. September 2014, Az. 4 LB 20/13) ist die Betreiberin oder der Betreiber einer Facebook-Fanpage für die allein von Facebook vorgenommene Verarbeitung personenbezogener Daten von Besucherinnen und Besuchern der Fanpage datenschutzrechtlich nicht verantwortlich. Sie oder er habe keinen Einfluss auf die technische und rechtliche Ausgestaltung der Datenverarbeitung durch Facebook. Dass sie oder er von Facebook anonyme Statistikdaten über Nutzerinnen und Nutzer erhalte, begründe keine datenschutzrechtliche Mitverantwortung (siehe auch die Pressemitteilung des OVG Schleswig-Holstein vom 05.09.2014). Gegen die Entscheidung wurde von der Beklagten Revision beim Bundesverwaltungsgericht eingelegt, das hierzu im Februar 2016 den EuGH angerufen hat, da es in dieser Angelegenheit um die Auslegung der Europäischen Datenschutzrichtlinie 95/46/EG geht. Die Entscheidung steht noch aus.

Die Landesregierung ist in Bezug auf Facebook keine datenverarbeitende Stelle im Sinne des § 3 NDSG. Dies würde voraussetzen, dass das jeweilige Ministerium selbst personenbezogene Daten verarbeitet oder durch andere im Auftrag verarbeiten lässt. Dies ist nicht der Fall. Nichtsdestotrotz weist die Landesregierung auf den von ihr betriebenen Facebook-Seiten der Ministerien die Nutzerinnen und Nutzer von Facebook explizit auf den vielfach zu Recht kritisierten Umgang des Unternehmens mit personenbezogenen Daten hin. Es wird beispielsweise darauf hingewiesen,

– dass Facebook nicht nur Daten speichert, die direkt von Nutzerinnen und Nutzern eingegeben werden, sondern auch Aktionen der Facebook-Nutzerinnen und -Nutzer - vermutlich lückenlos - aufzeichnet und so deren Vorlieben, Neigungen und Kontakte sehr genau und über die Facebook-Nutzung hinaus untersuchen kann, und

– dass bei jedem Besuch auf Webseiten, auf denen ein „Gefällt mir“-Knopf installiert ist, die IP-Adresse übertragen wird.

Sogenannte „gefällt mir“-Buttons sind auf den Seiten der Landesregierung nicht enthalten.

Die Facebook-Seiten der Landesregierung sind nur über einen Link auf den jeweiligen Webseiten zu erreichen. Bevor die Nutzerinnen und Nutzer auf die Facebook-Seite gelangen, werden Datenschutzhinweise angezeigt. Darüber hinaus sind die Facebook-Seiten öffentlich, d. h. interessierte Bürgerinnen und Bürger und Medienvertreterinnen und -vertreter müssen sich nicht bei Facebook anmelden, um Einträge lesen zu können.

Für den Umgang mit sozialen Medien in Behörden hat MI im Jahr 2012 einen Behördenleitfaden erstellt, der u. a. auf die Risiken von sozialen Medien wie Facebook hinweist. Der Leitfaden beschreibt Verhaltensregeln bei Behördenauftritten in Social Media und somit auch, ob und unter welchen Rahmenbedingungen ein Auftritt bei Facebook erfolgen kann.

In dieser Form hält die Landesregierung die Nutzung von Facebook-Seiten als zusätzliches Informationsangebot für vertretbar. Die Landesregierung begrüßt die politische Auseinandersetzung sowohl auf nationaler als auch auf europäischer Ebene mit der Praxis von Facebook. Um mehr Transparenz über den Umgang von Facebook mit personenbezogenen Daten zu erlangen und dies rechtlich bewerten zu können, haben Gespräche mit Vertreterinnen und Vertretern der Datenschutzressorts der Länder, der Aufsichtsbehörden für den Datenschutz und von Facebook stattgefunden. Die dabei erzielten Erkenntnisse sollen zu mehr Rechtssicherheit bei der Nutzung von Facebook beitragen.

Auch die Zulässigkeit der Nutzung sozialer Netzwerke wird künftig nach der Datenschutz-Grundverordnung zu bewerten sein. Die Verordnung wird sowohl für die Unternehmen mit Sitz innerhalb der EU gelten wie auch für Unternehmen mit außereuropäischem Sitz, soweit sie ihre Dienstleistungen Personen innerhalb der EU anbieten.

Feuerwehreinsätze auf Facebook

(TB, Seiten 136 bis 137)

Die LfD hat in ihrem Tätigkeitsbericht zu den Auftritten von freiwilligen Feuerwehren bei Facebook Stellung genommen und darauf hingewiesen, dass im Internet Bilder und Einsatzörtlichkeiten zu sehen waren, die einen unmittelbaren Personenbezug ermöglicht haben. Die LfD weist darauf hin, dass auch bei textlichen Informationen zu dem Einsatzgeschehen der Feuerwehr kein Personenbezug herstellbar sein darf. Bei der Veröffentlichung von Fotos ist darauf zu achten, dass grundsätzlich nur von öffentlich zugänglichen Bereichen foto- und videografiert werden darf. Bei der Veröffentlichung des Materials weist die LfD auf die rechtlichen Grenzen des § 22 Kunsturhebergesetz hin.

Die Hinweise und datenschutzrechtlichen Bedenken der LfD werden von der Landesregierung unterstrichen.

Im Rahmen der Novellierung soll aus diesem Grunde § 12 Abs. 4 des Niedersächsischen Brandschutzgesetzes, der die Pflichten der Angehörigen der freiwilligen Feuerwehr regelt, um die Pflicht zur Verschwiegenheit ergänzt werden. Diese Pflicht soll sich sowohl auf die Weitergabe von Kenntnissen als auch auf die Weitergabe von Fotos an die Öffentlichkeit beziehen. Die Erteilung von Auskünften an die Presse und die Weitergabe von Bildern jeglicher Art von der Einsatzstelle soll eine von der Gemeinde bestimmte Person vornehmen. Ein Verstoß gegen diese Pflicht soll als Ordnungswidrigkeit geahndet werden.

Im Zuge der Novellierung ist auch beabsichtigt, Empfehlungen im Zusammenhang mit den Veröffentlichungen der von Feuerwehrangehörigen gefertigten Fotos und Filmaufnahmen auszusprechen.

Darüber hinaus ist die Presse- und Öffentlichkeitsarbeit auch ein Bestandteil verschiedener Lehrgänge an der Niedersächsischen Akademie für Brand- und Katastrophenschutz, in welchen die Teilnehmerinnen und Teilnehmer auch für die datenschutzrechtlichen Belange sensibilisiert werden.

Der Heartbleed-Bug - Sicherheitslücke im Sicherheitsprotokoll

(TB, Seiten 146 bis 147)

Die LfD berichtet über ihre Prüfung im Zusammenhang mit der Feststellung von Sicherheitslücken auf Servern in Niedersachsen.

Die ersten Informationen über die Sicherheitslücke wurden am 07.04.2014 veröffentlicht. Am 08.04.2014 hat das Niedersächsische Computer Emergency Response Team (N-CERT) nach Verifikation die Dienststellen der niedersächsischen Landesverwaltung und die IT-Dienstleister darüber informiert. Am 10.04.2014 wurde die Lücke zentral auf dem Application Security Gateway (Siche-

rungskomponente des zentralen Internetzugangs) für alle Anwendungen, die darüber im Internet zur Verfügung gestellt werden, geschlossen. Das N-CERT überprüft kontinuierlich mit Unterstützung des Deutschen Forschungsnetzes DFN-CERT und CERT-Bund die Webseiten der niedersächsischen Landesverwaltung hinsichtlich bekannter Sicherheitslücken im SSL-Protokoll und informiert gegebenenfalls die betroffenen Dienststellen.

Die Sicherheitslücke im OpenSSL zeigt, dass mit der Offenheit von Softwarequellen keine Aussage über die Qualität und damit auch der Sicherheit der Software getroffen werden kann. Bei Open Source erscheint es zudem schwieriger, Qualitätsstandards einzuhalten, da jeder an den Codequellen Änderungen vornehmen kann. Auch kann niemand aufgrund schlechter Codequalität aus der Entwicklergemeinschaft ausgeschlossen werden.

Landesprojekt MDM

(TB, Seiten 159 bis 161)

Die LfD stellt die Situation der Entwicklung eines Landesprojektes zum Mobile Device Management (MDM) im Wesentlichen zutreffend dar. Dies gilt insbesondere für die Darstellung der widerstreitenden Interessen zwischen einem höheren Sicherheitsniveau und mehr Anwendungskomfort. Die kritische Begleitung des notwendigen weiteren Entwicklungsprozesses einer den aktuellen Anforderungen gerechten Lösung durch die LfD wird ausdrücklich begrüßt.

Informationssicherheit - Privacy by Design und Privacy by Default

(TB, Seiten 163 bis 164)

Im Tätigkeitsbericht wird die Bedeutung der Ansätze „Privacy by Design“ und „Privacy by Default“ betont, die bei allen IT-Planungen sowie in der Entwicklung und im Betrieb von IT-Verfahren Berücksichtigung finden sollten.

Insbesondere der Ansatz „Privacy by Design“ wird von der Landesregierung grundsätzlich begrüßt. Da allerdings in der Landesverwaltung vergleichsweise wenig Software-Entwicklung erfolgt, ist der Einfluss auf das Design von Software begrenzt. Das MI hat im Jahr 2012 einen Leitfaden für die Architektur von IT-Anwendungen in der niedersächsischen Landesverwaltung erstellt, der unter Ziffer 2.23 auch Aussagen zur Berücksichtigung des Datenschutzes beinhaltet. Zurzeit stellt der Leitfaden eine ausreichende Grundlage für IT-Architekturentscheidungen dar. Eine Überarbeitung ist daher nicht vorgesehen. Wenn aufgrund der Fortentwicklung der IT zukünftig doch eine Überarbeitung erforderlich sein sollte, soll der Ansatz „Privacy by Design“ in die Überarbeitung mit einfließen.

Mehr Personal für N-CERT

(TB, Seite 164)

Die LfD betont die zentrale Bedeutung des N-CERT für die Abwehr und Koordinierung von IT-Sicherheitsvorfällen und die Erforderlichkeit einer ausreichenden Ausstattung dieser Stelle mit Personal.

Diese Auffassung wird von der Landesregierung geteilt. Daher sind die Bemühungen, entsprechend qualifiziertes Personal für das N-CERT zu rekrutieren, nochmals intensiviert worden. Derzeit sind eine Mitarbeiterin und drei Mitarbeiter im N-CERT beschäftigt. Für die vakante fünfte Stelle haben im Februar 2016 Bewerbungsgespräche stattgefunden. Es ist davon auszugehen, dass die fünfte Stelle bis zum Jahresende besetzt sein wird.

Elektronische Aktenführung

(TB, Seiten 167 bis 168)

Bei der Einführung der elektronischen Aktenführung sieht die LfD im Zusammenhang mit weiteren Verwaltungsmodulen bei der Produktauswahl das Risiko der Produktabhängigkeit.

Die elektronische Aktenführung ist die Basis für eine medienbruchfreie digitale Gestaltung der Verwaltungsarbeit. Das Projekt eAkte orientiert sich entsprechend dem Kabinettsbeschluss aus 2012 am „Organisationskonzept elektronische Verwaltungsarbeit“ und den Empfehlungen in der „Referenzarchitektur elektronische Verwaltungsarbeit“. Beide Konzepte empfehlen sowohl organisato-

risch wie technisch eine Modularisierung, die den Austausch von Komponenten und die Zusammensetzung der Lösungen vereinfacht. Dieser Empfehlung folgend basiert die derzeitige Pilotlösung auf den Produkten MS Sharepoint und bonnea und somit auf zwei unterschiedlichen Produkten und Herstellern. MI geht davon aus, dass für die noch zu entwickelnden bzw. zu integrierenden Module der elektronischen Verwaltungsarbeit wie z. B. eVorgangsbearbeitung, eZusammenarbeit, Scannen, ePoststelle weitere Produkte unterschiedlicher Hersteller infrage kommen. Auf diese Weise kann Vorsorge zur Vermeidung einer Produkt- und Herstellerabhängigkeit getroffen werden.

MI wird bei der der Gestaltung der elektronischen Verwaltungsarbeit gemeinsam mit IT.Niedersachsen in enger Abstimmung mit der LfD ausführliche datenschutzrechtliche Risikobetrachtungen für die einzelnen Services und Lösungen durchführen. Ziel ist es, das Sicherheitsniveau in der Dokumentenverwaltung deutlich zu erhöhen. Zu dem jetzt in Vorbereitung befindlichen Basismodul eAkte hat im Oktober 2015 ein erstes Informationsgespräch mit der LfD stattgefunden.

Ende-zu-Ende-Verschlüsselung

(TB, Seite 168)

Dieser Abschnitt des Tätigkeitsberichts steht im Kontext der neuen Telekommunikations-Infrastruktur, der elektronischen Aktenführung und der verschlüsselten E-Mail-Kommunikation zwischen den technischen Übertragungsstellen. Im Tätigkeitsbericht wird eine von der Nutzerin oder dem Nutzer kontrollierte Ende-zu-Ende-Verschlüsselung als unabdingbar angesehen. Bei dieser generell gehaltenen Forderung sind jedoch nach Auffassung von MI zahlreiche technisch-organisatorische Anforderungen in Betracht zu ziehen, die beim Verfahrenseinsatz neben den fachlichen Anforderungen aus dem Verwaltungsprozess beachtet werden müssen. Beispielsweise muss geklärt werden, wer der Empfängerkreis von verschlüsselten Nachrichten ist und wie dort damit umgegangen werden soll (innerhalb oder außerhalb der Landesverwaltung), wie es mit der Schlüsselübergabe und -verwaltung bestellt sein soll, welche Anforderungen an die Durchsuchbarkeit von verschlüsselten Nachrichten gestellt werden, welche Schutzmaßnahmen bei gleichfalls verschlüsselter Schadsoftware in verschlüsselten Nachrichten getroffen werden müssen oder wie die elektronische Aktenführung bei verschlüsselten Nachrichten zu gestalten ist u. a. m.

Produkte für eine Ende-zu-Ende-Verschlüsselung von E-Mail-Nachrichten stehen zahlreich auf dem Markt zur Verfügung und wurden und werden in unterschiedlichen Behörden der Landesverwaltung erprobt. Erfolgreich werden diese Produkte nur dann eingesetzt werden können, wenn die oben beispielhaft genannten technisch-organisatorischen Anforderungen festgelegt worden sind. MI plant dazu die in der Vergangenheit begonnenen Ansätze aufzugreifen und fortzuentwickeln.

Informationssicherheitsrichtlinie E-Mail

(TB, Seiten 169 bis 171)

In ihrem Bericht bemängelt die LfD, dass ein in der Entwurfsfassung der Informationssicherheitsrichtlinie (ISRL) E-Mail-Nutzung vorgesehenes ausdrückliches Verbot des Versands von Daten der Schutzstufen D und E im Anschluss wieder gestrichen wurde.

Weder in früheren Regelungen noch in dem am 23.10.2013 für die 14. Sitzung des Niedersächsischen IT-Planungsrats vorgelegten Entwurf der ISRL E-Mail-Nutzung war ein Verbot des Versands von Daten der Schutzstufe D per E-Mail enthalten.

Die Landesregierung teilt die Einschätzung der LfD, dass der Versand von Daten mit hohem und sehr hohem Schutzbedarf umfangreicher technischer und organisatorischer Maßnahmen zum Schutz der per E-Mail übertragenen Informationen erfordert. Die Landesregierung ist ebenfalls der Ansicht, dass die konkrete Ausgestaltung der technisch-organisatorischen Maßnahmen am jeweiligen Schutzbedarf der elektronisch übermittelten Informationen auszurichten ist. Hierzu sind gemäß der Informationssicherheitsleitlinie (ISLL) entsprechende Risikoanalysen durchzuführen und die bestehenden Risiken, die in der Eintrittswahrscheinlichkeit und dem Schadensausmaß insbesondere die Aspekte des Schutzbedarfs abbilden, auf ein verantwortbares Maß zu reduzieren. Dies soll in erster Linie durch technische Maßnahmen erfolgen.

Die im Bericht dargelegten „möglichen Angriffe von außen und innen“ bekräftigen beispielhaft dieses Vorgehen. Entsprechend trägt die Ziffer 5.5.1 der ISRL E-Mail-Nutzung der Forderung nach ei-

ner dem jeweiligen Schutzbedarf der Informationen angemessenen Verschlüsselung Rechnung. Die Orientierungshilfe „Verschlüsselung“ der LfD fand im Entstehungsprozess dieser ISRL umfassende Berücksichtigung.

Ein im Entwurf der ISRL E-Mail-Nutzung vom 23.10.2013 vorgesehenes Verbot des E-Mail-Versands von Daten der Schutzstufe E wurde auf Wunsch mehrerer Ressorts in die Rege-lungen der risikobasierten Beurteilung und Maßnahmenplanung überführt. Der Vorteil dieser Neuregelung ist die Flexibilität bei der sukzessiven Beschaffung oder Herstellung von ausreichend sicheren Lösungen bei voller Verantwortungsübernahme der Behördenleitungen. Der ISLL entsprechend war es die Entscheidung aller Ressorts, keine zentrale Entscheidung über die absolute Unzulässigkeit der Verarbeitung von Daten der Schutzstufe E zu treffen. Die Behördenleitungen sind vielmehr zur Risikoanalyse unter Berücksichtigung der Eintrittswahrscheinlichkeit und des Schadensausmaßes (Schutzbedarfs) und zur Ermittlung angemessener Lösungen zur Risikoreduzierung oder gegebenenfalls zur Risikovermeidung durch Funktionsbeschränkungen (s. Nrn. 4.3/5.2 ISLL) verpflichtet worden.

Die Entscheidung über die Verabschiedung der ISRL E-Mail-Nutzung ist am 30.07.2014 einstimmig durch den Niedersächsischen IT-Planungsrat getroffen worden. Die ISRL ist als gemeinsamer Runderlass des MI, der StK und der übrigen Ministerien veröffentlicht worden.

Dem überwiegenden Wunsch der Ressorts entsprechend enthält der Runderlass als Anlage eine Musterdienstanweisung. Diese Orientierungshilfe unterstützt die Organisationsverantwortung der Behördenleitung und stellt beispielhaft Umsetzungsvarianten für die behördenspezifische Dienstanweisung, mit denen die Mindestanforderungen der ISRL eingehalten werden, dar. Die Behördenleitung kann so organisatorische Regelungen verfügen, die den Bediensteten eine geringere Mitwirkung abverlangen, wenn dies z. B. durch technische Lösungen ermöglicht wird und die Einhaltung der ISRL dadurch garantiert ist.

Technische Lösungen können Gefahrenpotenziale jedoch immer nur bis zu einem gewissen Grad reduzieren. Der Versand von E-Mails wird jedoch immer willentlich durch die Anwenderin oder den Anwender gesteuert, ohne deren erforderliche Fertigkeiten und Aufmerksamkeit würde gerade beim E-Mail-Einsatz schwerlich ein vertretbares Sicherheitsniveau erreicht werden können.

Eine „Überforderung der Anwenderinnen und Anwender“ kann sich durch die Musterdienstanweisung nicht ergeben, weil sich eine ISRL einschließlich der anhängenden Musterdienstanweisung ausschließlich an die Behördenleitung richtet. Der Behördenleitung obliegt die adressatengerechte Ausgestaltung der Dienstanweisung an die Anwenderinnen und Anwender im Zusammenspiel mit technischen und organisatorischen Maßnahmen, sodass die Anwenderinnen und Anwender beim Umgang mit Daten höheren Schutzbedarfs nicht überfordert werden.

Nicht nachvollzogen werden kann in diesem Zusammenhang die Folgerung auf Seite 171 des Berichts: „Wie die Musterdienstanweisung deutlich macht, ist die Landesverwaltung auch nach Einführung des Niedersachsenclients (siehe Seite 172: Windows 8.1 in der Landesverwaltung) nicht in der Lage, Angriffe durch Schadprogramme auf technischem Wege zuverlässig zu verhindern.“

Windows 8.1 in der Landesverwaltung

(TB, Seiten 172 bis 174)

Die LfD bemängelt in ihrem Bericht das Verfahren bei der Einstellung von Windows XP und der Einführung der Version Windows 8.1.

Sowohl die Darstellung des Sachverhalts zur Einführung von MS-Windows 8.1 als auch die Schlussfolgerungen hierzu können seitens der Landesregierung nicht nachvollzogen werden.

Das Outsourcingprojekt für das Desktopmanagement von ca. 8 000 IT-Arbeitsplätzen ist im Jahr 2013 im gegenseitigen Einvernehmen beendet worden. Auf Basis der Kabinettsbeschlüsse vom 23.06.2013 und vom 03.12.2013 hat IT.N den Auftrag erhalten, auf den o. a. IT-Arbeitsplätzen sowohl die Hardware als auch die Software zu erneuern. Bestandteil dieses Auftrags war es, die Produkte der Fa. Microsoft für das Betriebssystem (MS-Windows) und die Bürokommunikation (MS-Office) zu verwenden. Der Niedersächsische IT-Planungsrat hat diesen Auftrag mit Beschluss vom

23.10.2013 dahin gehend konkretisiert, dass die Produktversionen MS-Windows 8.1 und MS-Office 2013 eingesetzt werden sollten.

Der Umstieg auf andere Produktlinien wie z. B. Linux/Libre Office kam seinerzeit aus strategischen Gründen nicht in Betracht. Andere Migrationsprojekte (wie z. B. bei der Stadt München) haben gezeigt, dass die Migrationsaufwände enorm, wenn nicht gar unbeherrschbar sind, da auch die Fachverfahren zum Teil migriert werden müssen. Die Erfahrungen bei der Polizei haben zudem gezeigt, dass mit einer reinen Open Office-Plattform die fachlichen Anforderungen vielfach nicht erfüllt werden können, sodass dort dezentral zusätzliche Windows-Systeme aufgebaut wurden. Da dies weder aus wirtschaftlichen noch aus sicherheitstechnischen Gründen zielführend ist, hat sich die Polizei für eine Abkehr von der Linux-Welt entschieden.

Durch die Beendigung des Outsourcingvertrages war das Modernisierungsprojekt um ca. ein Jahr in Verzug geraten. Dadurch konnte die von der Fa. Microsoft gesetzte Frist für das Ende des kostenfreien Supports (08.04.2014) der Produkte MS-Windows XP und MS-Office 2003 nicht eingehalten werden. Microsoft bot jedoch für diejenigen Kundinnen und Kunden, die den Umstieg auf eine neuere Produktversion planten, einen fortlaufenden kostenpflichtigen Support an. Das Land Niedersachsen hat hierzu einen entsprechenden Vertrag geschlossen, um drohende Sicherheitslücken zu schließen.

Die Darstellung im Tätigkeitsbericht, dass durch den Supportvertrag das Land gezwungen worden wäre, weiterhin Microsoft-Produkte einzusetzen, verdreht Ursache und Wirkung. Es ist in der Softwareindustrie absolut üblich, dass nur für einen bestimmten Zeitraum Produktsupport erhältlich ist („Life Cycle“). Es ist auch unter Sicherheitsaspekten sinnvoll, nach einem gewissen Zeitraum die Produkte vom Markt zu nehmen und vollständig neu zu entwickeln. Für Windows XP wurde der kostenfreie Support immerhin 13 Jahre bereitgestellt. Das Supportende wurde mit fünf Jahren Vorlauf bekannt gegeben. Die Notwendigkeit zum Abschluss des kostenpflichtigen Supportvertrages ergab sich allein durch die o. a. Verzögerung des Modernisierungsprojekts. Zum Zeitpunkt des Abschlusses des Supportvertrages war die Entscheidung, weiterhin Microsoft-Produkte einzusetzen, bereits getroffen worden (siehe oben).

IT.Niedersachsen hat in Abstimmung mit der LfD seinerzeit eine ausführliche datenschutzrechtliche Risikobetrachtung durchgeführt. Diese hatte zum Ergebnis, dass sich durch den Einsatz der neuen Produkte das Sicherheitsniveau deutlich erhöht hat. Zusätzliche Risiken, die sich durch neue Funktionen hätten ergeben können, wurden durch Deaktivierung minimiert (z. B. Microsoft-Konto, OneDrive).

Gefahren durch Internetdienste und Sicherheitslücken/Sicherheitsdomänen und Virtualisierung

Die Erkenntnis der LfD, dass die Entwicklung der Anzahl und Art der Bedrohungen aus dem Cyberraum in den letzten Jahren ein geändertes Vorgehen erfordert, wird geteilt. Neben der Verbesserung der angesprochenen etablierten Sicherheitstechnologien, Virenscannern und Update-Versorgung befasst sich das MI seit 2012 mit der Einführung neuartiger Sicherheitsmethoden, insbesondere mit dem „Intrusion Detection System“ (IDS) und „Security Information- and Event-Management“ (SIEM)-Systemen. Hierbei stehen der Chief Information Security Officer und das N-CERT in enger Zusammenarbeit mit der LfD, da die neuen Technologien zwar vielfältige gewünschte Sicherheitsverbesserungen ermöglichen, daneben aber umfangreiche rechtliche Betrachtungen im Bereich des Datenschutzes, des Telekommunikationsrechts, des Telemedienrechts und des Personalvertretungsrechts notwendig machen. Die IDS- und SIEM-Technologie stellen in Zusammenhang mit der Einrichtung des N-CERT zwei neue Säulen der Informationssicherheitsarchitektur dar, die die etablierten Einrichtungen des Perimeterschutzes und der musterbasierten Erkennung von Viren ergänzen und neu einordnen. Als weiterer Baustein wird die Einführung von virtualisierten Umgebungen geplant, die die von der LfD angeführte Kapselung riskanter Abläufe von den Wirtssystemen ermöglicht.

„Microsoft erhält persönliche Daten der Beschäftigten“

Die Darstellung im Bericht, dass mit der Einführung von MS-Windows 8.1 und MS-Office 2013 die personenbezogenen Daten der Beschäftigten an Microsoft übermittelt würden, kann nicht nachvollzogen werden. Wie oben dargestellt, wurden einerseits solche Funktionen deaktiviert, die auf ei-

nem Microsoft-Konto basieren. Ferner wird - auch auf Anregung der LfD - seit 2015 die Übermittlung der sogenannten XFF-Header am Proxy der Landesfirewall unterbunden, sodass - beispielsweise bei der Nutzung der Online-Hilfe - ein Rückschluss auf einzelne Beschäftigte nicht mehr möglich ist. Indirekte Identifizierungsmöglichkeiten sind bei jeglicher Nutzung des Internets theoretisch möglich und zählen zu den Restrisiken. Diese haben jedoch keinen ursächlichen Zusammenhang mit der Einführung von MS-Windows 8.1 und MS-Office 2013.

Für den hier konkret angesprochenen Datenabfluss durch Nutzung der Hilfefunktionen wurde zudem ein umfangreiches Schulungsprogramm aufgesetzt, welches u. a. die Installation eines Hilfe-Programms der Fa. Soluzione umfasste. Diese Software wurde in das Betriebssystem und die Office-Komponenten als „Add-In“ integriert und hat einen wesentlich größeren Funktionsumfang (Tutorials, Umstiegshilfen von Office 2007 auf 2013 u. v. m.) als die normale Hilfefunktionalität von Microsoft. Dadurch wurde die Notwendigkeit, überhaupt auf die Online-Hilfe zuzugreifen, auf ein Minimum reduziert.

E-Mailverkehr in der Justizverwaltung

(TB, Seiten 182 bis 183)

Die LfD verweist auf die Gefahren, die bei der Übermittlung von Daten per E-Mail entstehen können. Dies gilt insbesondere für sensible Daten höherer Schutzstufen. Hier sei es zwingend erforderlich, eine Übermittlung ausschließlich unter Einsatz einer Ende-zu-Ende-Verschlüsselung vorzunehmen. Im Bereich der Kommunikation zwischen der Justizverwaltung und der Polizei standen zum Berichtszeitpunkt die von der LfD angeforderten Nachweise eines ausreichenden Schutzes der Daten noch aus.

Im Bereich der niedersächsischen Justiz war bereits in der Dienstanweisung für die Nutzung der elektronischen Post (Electronic-Mail nach X.400) im Geschäftsbereich des MJ vom 17.05.2001 geregelt, dass die elektronische Übermittlung von sensiblen und schutzwürdigen Daten insbesondere der Schutzstufen D und E bis zum Vorliegen einer gesonderten verbindlichen Verfahrensweise zur Verschlüsselung der Datenübertragung nicht zulässig ist.

Diese grundsätzliche Unzulässigkeit der elektronischen Übermittlung wurde mit Erlassen vom 26.09.2012 und 12.11.2012 für personenbezogene Daten der Schutzstufen D und E zunächst für den Bereich innerhalb der niedersächsischen Justiz aufgehoben. Mit Erlass vom 26.06.2013 erfolgte die Aufhebung für die Kommunikation mit der niedersächsischen Polizei. Im Vorfeld der Erlasse zur Erweiterung der Zulässigkeit des E-Mailversandes innerhalb der niedersächsischen Justiz wurde ein Sicherheitskonzept des Zentralen IT-Betriebs Niedersächsische Justiz (ZIB) für den sicheren E-Mailversand angefertigt. Der ZIB betreibt die IT für die niedersächsische Justiz. Dazu gehören u. a. die eigenen E-Mailserversysteme und Clients. Die flächendeckende Einführung der Transport Layer Security (TLS)-Verschlüsselung für den E-Mailtransport zwischen den Clients und den Serversystemen sowie auch zwischen den beteiligten Serversystemen stellt nach Einschätzung des MJ eine Verfahrensweise zur Verschlüsselung der Datenübertragung im Sinne der o. g. Dienstanweisung dar. Die Ausweitung der E-Mailkommunikation wurde daher durch die mit dem behördlichen Datenschutzbeauftragten abgestimmten Erlasse aus dem Jahr 2012 dem Geschäftsbereich des MJ bekanntgegeben.

Nach Abstimmung mit MI und der Zentralen Polizeidirektion Niedersachsen (ZPD) wurde die Zulässigkeit der elektronischen Übermittlung auf den Bereich der niedersächsischen Polizei mit dem o. g. Erlass aus dem Jahr 2013 erweitert. Zur technischen Umsetzung wurden die jeweiligen TLS-Verschlüsselungszertifikate zwischen ZPD und ZIB ausgetauscht und durch gegenseitige Akzeptanz dieser Zertifikate ein gemeinsamer Transportverschlüsselungsraum hergestellt.

Im Bereich der Polizei erfolgt beim Versenden einer E-Mail durch eine Mitarbeiterin oder einen Mitarbeiter innerhalb der Polizei zunächst ein Verbindungsaufbau zum Server der jeweiligen Polizeibehörde. Im Anschluss erfolgt ein Verbindungsaufbau durch den Server der Polizeibehörde, von dem die E-Mail versandt werden soll, zum Server der Polizeibehörde, in der die Empfängerin oder der Empfänger organisatorisch zugeordnet ist. Während der Versand der E-Mail durch eine Transportverschlüsselung gegen unbefugte Einsichtnahme geschützt wird, erfolgt die Speicherung der E-Mails auf den Servern ohne eine Verschlüsselung. Beim Versand einer E-Mail zu einer externen E-

Mailadresse wird die E-Mail vom Server der jeweiligen Polizeibehörde über IT.Niedersachsen unverschlüsselt an die jeweilige Empfängeradresse übermittelt.

In der Ressortabstimmung zur ISRL E-Mail-Nutzung im zweiten Halbjahr 2013 und dem darin formulierten geplanten generellen Versandverbot von personenbezogenen Daten der Schutzstufe E sind MI und MJ darin übereingekommen, die Praxis der Freigabe der transportverschlüsselten E-Mail-Kommunikation mit personenbezogenen Daten der Schutzstufen D und E durch die LfD überprüfen zu lassen. Hierzu wurde die ZPD durch MI beauftragt, eine Vorabkontrolle nach § 7 Abs. 3 NDSG zu erstellen und diese dann an die LfD zur Stellungnahme weiterzuleiten. Die Vorabkontrolle wurde am 30.11.2014 erstellt und MJ nach Übersendung der Stellungnahme der LfD am 13.07.2015 zur Kenntnisnahme übersandt.

Die Vorabkontrolle durch die ZPD hatte ergeben, dass die eingerichtete Transportverschlüsselung für den Versand von sensiblen und schutzbedürftigen personenbezogenen Daten per E-Mail innerhalb der Polizei und im Austausch mit den Justizbehörden des Landes Niedersachsen bis Schutzstufe D, jedoch nicht darüber hinaus, zulässig sei. Dieser Bewertung widersprach die LfD mit der Begründung, dass diese technischen Sicherheitsvorkehrungen nicht ausreichend seien, um Möglichkeiten einer Fehladressierung durch den Absender der E-Mail, z. B. durch Autovervollständigung oder Tippfehler, entgegenwirken zu können, wenn Daten der Schutzstufe D versandt werden sollen. Hierfür sei die Einrichtung einer Ende-zu-Ende-Verschlüsselung für den Mailversand zwischen der Polizei und den Justizbehörden zwingend erforderlich, um den Schutz des sensiblen Kommunikationsinhaltes gewährleisten zu können.

Die Einschränkung der Vorabkontrolle auf Daten der Schutzstufe D war MJ bis dahin nicht bekannt. Als Reaktion auf die Stellungnahme der LfD zur Vorabkontrolle wurde am 28.07.2015 durch MJ eine Anfrage an MI zur Suche einer landesweiten Lösung für die Ende-zu-Ende-Verschlüsselung gestellt.

Da auch seitens der Polizei der Bedarf besteht, neben den Justizbehörden auch mit weiteren berechtigten Dritten sensible Daten bis Schutzstufe D per E-Mail zu kommunizieren und dieser Bedarf auch in anderen Ressorts des Landes Niedersachsen vermutet wird, wurde IT.Niedersachsen im Juni 2015 gebeten, bis zum Ende des Jahres auf Basis dieses Bedarfes unter Berücksichtigung der Anforderungen der LfD an eine Ende-zu-Ende-Verschlüsselung einen Produktvorschlag zu unterbreiten, der unter Umständen dann landesweit zum Einsatz kommen könnte. Im November 2015 erfolgte hierzu eine Besprechung zwischen IT.Niedersachsen, MI sowie den Justizbehörden, deren Ergebnis es war, die funktionalen Anforderungen der Polizei und der Justiz zu konkretisieren, um IT.Niedersachsen in die Lage zu versetzen, einen Produktvorschlag zu unterbreiten. Die Arbeiten hierzu dauern aktuell noch an.

Als Reaktion auf die o. g. Stellungnahme der LfD wurde seitens MJ mit Erlass vom 19.10.2015 der E-Mail-Versand von personenbezogenen Daten der Schutzstufe E wieder für unzulässig erklärt. Darüber hinaus wurde der Versand von Daten der Schutzstufe D an die niedersächsische Polizei nur mit einer Ende-zu-Ende-Verschlüsselung der E-Mails gestattet. Innerhalb der niedersächsischen Justiz ist der E-Mail-Versand von Daten der Schutzstufe D weiterhin mit TLS-Transportverschlüsselung zulässig.

Den von der LfD vorgebrachten Risiken und Gefahren wird durch die aktuell gültigen Einschränkungen zur Zulässigkeit der elektronischen Übermittlung von personenbezogenen Daten der Schutzstufen D und E Rechnung getragen.

Ein Informationszugangs- und Transparenzgesetz für Niedersachsen

(TB, Seiten 190 bis 194)

Derzeit verfügt Niedersachsen noch über kein Informationsfreiheitsgesetz. In der Koalitionsvereinbarung, die SPD und Bündnis 90/Die Grünen im Februar 2013 für die 17. Wahlperiode des Niedersächsischen Landtages geschlossen haben, ist jedoch festgehalten, dass die rot-grüne Koalition ein Landes-Informationsfreiheitsgesetz verabschieden wird. Die entsprechenden Passagen auf Seite 70 und 80 des Koalitionsvertrages lauten: „Die rot-grüne Koalition wird ein Landes-Informationsfreiheitsgesetz beschließen. Sie orientiert sich dabei am Hamburger Transparenzgesetz.“ sowie „Die rot-grüne Koalition wird endlich auch in Niedersachsen eine umfassende Open-

Data-Strategie mit einem modernen Informationsfreiheits- und Transparenzgesetz vorlegen. Es soll staatliche Stellen verpflichten, alle relevanten Informationen digital in einem Transparenzregister zu veröffentlichen. Nur in begründeten Ausnahmetatbeständen - so zum Schutz von personenbezogenen Daten oder zum Schutz öffentlicher Belange - soll der Informationszugang im Einzelfall verwehrt bleiben."

Mit der Erarbeitung eines entsprechenden Gesetzentwurfs hat die Landesregierung das MJ beauftragt. Dort wurde ein Referentenentwurf erarbeitet, der derzeit mit den übrigen Ministerien und weiteren obersten Landesbehörden abgestimmt wird.