Unterrichtung

Hannover, den 25.02.2019

Der Niedersächsische Ministerpräsident

Stellungnahme der Landesregierung zum 23. Bericht über die Tätigkeit der Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 2015 und 2016 (Drs. 18/1510)

Frau
Präsidentin des Niedersächsischen Landtages
Hannover

Sehr geehrte Frau Präsidentin,

als Anlage übersende ich die

> **Stellungnahme der Landesregierung zum 23. Bericht über die Tätigkeit der Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 2015 und 2016** (Drs. 18/1510).

Federführend ist das Ministerium für Inneres und Sport.

Mit freundlichen Grüßen

Stephan Weil

(Verteilt am 01.03.2019)

Stellungnahme der Landesregierung zum XXIII. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Niedersachsen 2015 - 2016
Inhaltsverzeichnis

Vorbemerkungen

Der Tätigkeitsbericht der Landesbeauftragten für den Datenschutz Niedersachsen (LfD) für die Jahre 2015 – 2016 befasst sich mit dem Datenschutz für den öffentlichen Bereich, für den nicht öffentlichen Bereich (Wirtschaftsbereich) und übergreifenden sowie besonderen Themen wie die Videoüberwachung. Außerdem kommt europäischen Themen wie der Datenschutzreform und internationalen Themen wie der Datenübermittlung in Drittstaaten immer mehr Bedeutung zu. Dem Berichtszeitraum liegt die Rechtslage vor der Geltung der Datenschutz-Grundverordnung und der Neufassung des niedersächsischen Datenschutzrechts zum 25.05.2018 zugrunde.

Gemäß § 22 Absatz 3 Satz 1 des Niedersächsischen Datenschutzgesetzes (NDSG) in der bis zum 24.05.2018 geltenden Fassung 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 Absatz 1 Satz 7 Bundesdatenschutzgesetz (BDSG), ebenfalls in der bis zum 24.05.2018 geltenden Fassung. Eine Stellungnahme der Landesregierung ist hierzu gesetzlich nicht vorgesehen. Für diesen Bereich wird daher – wie in den vergangenen Berichts-

zeiträumen - nur zu einzelnen ausgewählten Themen von besonderem Interesse oder bei ausdrücklicher Kritik der LfD Stellung genommen.

Europa und internationaler Datenverkehr

Europäische Datenschutzreform

(TB, Seiten 12 bis 18)

Mit jedem Tätigkeitsbericht nimmt die europäische Datenschutzreform mehr Raum ein. Die LfD beschreibt den Ablauf seit dem Jahr 2012, in dem die Europäische Kommission den Entwurf für eine Datenschutz-Grundverordnung (DSGVO) vorgelegt hat, bis zum Jahr 2016, in dem nach intensivsten Beratungen die Verordnung (EU) 2016/679 und die Datenschutz-Richtlinie (EU) 2016/680 für den Bereich der Polizei und Justiz in Kraft getreten sind.
Die Landesregierung begrüßt wie die LfD die Harmonisierung des europäischen Datenschutzrechts. Niedersachsen hat sich wie auch alle anderen Bundesländer und die Bundesregierung intensiv in den Beratungsprozess eingebracht. Insbesondere zu den nationalen Anpassungsaufgaben haben sich die Zusammenarbeit und der Austausch mit den anderen Bundesländern und dem Bund bewährt und in vielen Bereichen zu einheitlichen Verfahrensweisen und Rechtsauslegungen geführt.

In Niedersachsen wurden alle Ressorts von dem für das allgemeine Datenschutzrecht zuständigen federführenden Ministerium für Inneres und Sport im Vorfeld über den Anpassungsbedarf informiert und bei der Gesetzgebung sowie bei der Umsetzung beraten. Der überwiegende Teil der anzupassenden Vorschriften wurde in das Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts eingebracht, das neben diversen Fachvorschriften die Neufassung des NDSG enthält. Die LfD wurde bei dem Vorhaben von Anfang an umfassend beteiligt.

Polizei und Verfassungsschutz

Vorratsdatenspeicherung

(TB, Seiten 22 bis 24)

Die von der LfD dargestellte Rechtsauffassung zur derzeitigen Rechtslage in Deutschland wird von der Landesregierung geteilt. Danach dürften die §§ 113a-113g Telekommunikationsgesetz (TKG) mit dem EU-Recht nicht vereinbar sein. In seiner Entscheidung vom 21.12.2016 (C-203/15 und C-698/15) hat der Europäische Gerichtshof (EuGH) festgestellt, dass eine nationale Regelung, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmerinnen und Teilnehmer und registrierten Nutzerinnen und Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsieht, mit EU-

Recht nicht vereinbar sei. Zwar werden in Deutschland die Daten nicht so lange gespeichert, wie in den der EuGH-Entscheidung zugrunde liegenden Fällen. Aber auch § 113b TKG sieht eine allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten vor. So hat auch das Oberverwaltungsgericht Nordrhein-Westfalen mit Beschluss vom 22.06.2017 (13 B 238/17) einem IT-Unternehmen im einstweiligen Rechtsschutzverfahren dahingehend Recht gegeben, dass es zur Speicherung der Telekommunikationsverkehrsdaten seiner Kundinnen und Kunden nach § 113b TKG nicht verpflichtet sei, da diese Regelung europarechtswidrig sei. Vor dem Hintergrund dieser Entscheidung hat die Bundesnetzagentur angekündigt, keine Bußgelder gegen Unternehmen zu verhängen, die ihren Speicherpflichten nach §§ 113a ff. TKG nicht nachkämen.

Polizei

Gesetz über die öffentliche Sicherheit und Ordnung

(TB, Seiten 28 bis 29)

Die LfD thematisiert in ihrem Bericht den Entwurf der Landesregierung zur Novellierung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) vom 03.08.2016 (LT-Drs. 17/6232). Sie äußert Kritik zu den Personenkontrollen nach § 12 Abs. 6 Nds. SOG, zur verdeckten Videoüberwachung nach § 32 Abs. 2 Nds. SOG und zur Befugnisnorm für den Bodycam-Einsatz mit Tonfunktion. Darüber hinaus moniert sie die fehlenden bereichsspezifischen Zweckänderungs- und Löschvorschriften.

Der Entwurf der Landesregierung zur Novellierung des Nds. SOG ist wegen des vorzeitigen Endes der 17. Legislaturperiode nicht verabschiedet worden. Da die genannten Punkte auch im gegenwärtigen Entwurf der Fraktionen der SPD und der CDU zur Novellierung des Nds. SOG (LT-Drs. 18/850) enthalten sind, nimmt die Landesregierung hierzu wie folgt Stellung:

- Personenkontrollen nach § 12 Abs. 6 Nds. SOG sind ein in der Polizeipraxis wichtiges Mittel, um grenzüberschreitende Kriminalität zu bekämpfen. Sie werden auf der Grundlage von polizeilichen Lageerkenntnissen durchgeführt. Die Lageerkenntnisse basieren auf Tatsachen, die somit Anknüpfungspunkt für polizeiliche Maßnahmen sind. Eine Personenkontrolle erfolgt auf dieser Tatsachenbasis. Der Verhältnismäßigkeitsgrundsatz ist darüber hinaus eine allgemeine Maxime des polizeilichen Handelns, die auch bei diesen Personenkontrollen beachtet wird.
- Die verdeckte Videoüberwachung gemäß § 32 Abs. 2 Nds. SOG wird zu präventiven Zwecken genutzt, um erwartete Gefahrensachverhalte zu beobachten und rechtzeitig vor ihrer Eskalation einschreiten zu können. Bei offener Videoüberwachung kann es demgegenüber zu einer Verlagerung an andere, der Polizei nicht bekannte Orte kommen. Ein rechtzeitiges Einschreiten wäre dann nicht gesichert. Der Einsatz liegt damit

im Bereich der Gefahrenabwehr und der Straftatenverhütung, wofür der Landesgesetzgeber die Gesetzgebungskompetenz hat.

- Für die Datenverarbeitung und die Prüf-/Löschfristen im Bereich des Bodycam-Einsatzes gelten die allgemeinen Regelungen der §§ 38, 39 und 39a Nds. SOG sowie die Prüffristen nach § 47 Nds. SOG. Weitergehender Regelungen bedarf es aus Sicht der Landesregierung in diesem Fall nicht.
- Bereichsspezifische Regelungen zur Zweckänderung werden nicht für erforderlich gehalten. Hier genügt die Regelung in § 39 Nds. SOG sowie im Rahmen der Übermittlung die §§ 40 ff. Nds. SOG. Hinsichtlich der Löschung wird § 39a Nds. SOG im Zusammenspiel mit der turnusmäßigen Prüfung zur Speichererforderlichkeit nach § 47 Nds. SOG als ausreichend erachtet.

Telekommunikationsüberwachung

(TB, Seiten 32 bis 35)

Es besteht weiterhin das dringende Erfordernis, die Instrumente für die Erkenntnisgewinnung der Sicherheitsbehörden, u. a. bei der Telekommunikationsüberwachung (TKÜ), 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 Ausführungen der LfD zur TKÜ-Anlage des Landeskriminalamtes Niedersachsen (LKA NI) und zum Projekt Rechen- und Dienstleistungszentrum Telekommunikationsüberwachung der Polizei im Verbund der norddeutschen Küstenländer (RDZ TKÜ) sind im Hinblick auf den Zeitraum 2015 und 2016 zutreffend.

Die von der LfD beschriebenen Mängelpunkte zur TKÜ-Anlage des LKA NI werden, soweit technisch und fachlich umsetzbar, durch das LKA NI in einem kontinuierlichen Dialog mit der LfD weiterhin priorisiert betrachtet und bearbeitet. Die Abhängigkeit vom Dienstleister der Systemtechnik zur Telekommunikationsüberwachung ist hierbei in weiten Teilen maßgeblich. Das Projekt RDZ TKÜ steht zu aktuellen Entwicklungen in regelmäßigem Austausch mit der LfD.

Rechtswidriger Einsatz von Bodycams durch die Polizei

(TB, Seiten 36 bis 38)

Die LfD thematisiert in ihrem Tätigkeitsbericht die Rechtmäßigkeit des Einsatzes von Bodycams durch die Polizei zum Schutz vor gewalttätigen Übergriffen. Sie vertritt die Auffas-

sung, dass der Einsatz der Bodycams im Berichtszeitraum nicht auf § 32 Abs. 4 Satz 1 des Nds. SOG gestützt werden könne. Sie moniert darüber hinaus, dass nach § 7 Abs. 3 NDSG in der bis zum 24.05.2018 geltenden Fassung (NDSG a.F.) eine Vorabkontrolle vor dem Einsatz der Bodycams erforderlich gewesen sei, diese aber nicht stattgefunden habe.
Rechtsgrundlage zum Einsatz von Bodycams ist § 32 Abs. 4 Nds. SOG. Dort ist geregelt: „Die Polizei kann zur Eigensicherung bei Anhalte- und Kontrollsituationen im öffentlichen Verkehrsraum nach diesem Gesetz oder anderen Rechtsvorschriften Bildaufzeichnungen offen anfertigen. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden."
Diese Formulierung bietet neben dem Einsatz von Kameras in Kraftfahrzeugen auch die Möglichkeit, die Beamtinnen und Beamten zum Eigenschutz mit am Körper getragenen Kameras, den sog. Bodycams, auszustatten, die auf die Bildaufzeichnungsfunktion beschränkt sind. In diesem rechtlichen Rahmen werden die Bodycams derzeit in Niedersachsen eingesetzt.
Der Gesetzgebungs- und Beratungsdienst des Landtags hat in der 115. Sitzung des Ausschusses für Inneres und Sport am 23.03.2017 die Rechtsauffassung des Ministeriums für Inneres und Sport bezüglich der Rechtsgrundlage für den Einsatz von Bodycams ohne Tonaufnahmen und ohne die „pre-recording"-Funktion bestätigt. Dies ist der LfD bekannt.
Eine datenschutzrechtliche Vorabkontrolle hält die Landesregierung im vorliegenden Fall nicht für erforderlich, da es beim Einsatz der Bodycams weder um den Einsatz automatisierter Datenverarbeitungsanlagen nach § 7 Abs. 3 NDSG a.F. geht noch § 25a NDSG a.F. einschlägig ist, der die Videoüberwachung öffentlicher Räume regelt. Um die vertrauensvolle Zusammenarbeit mit der LfD fortzusetzen, wurde trotzdem eine Vorabkontrolle zugesagt, die nach umfangreichem Schriftwechsel mit der LfD schließlich im Jahr 2017 übersandt wurde.
Für den zukünftigen Einsatz von Bodycams mit Tonaufnahme und der Funktion „pre-recording" sind im Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze vom 08.05.2018 (LT-Drs. 18/850), der von den Fraktionen der SPD und der CDU in den Landtag eingebracht wurde, entsprechende Regelungen vorgesehen. Eine Beteiligung der LfD am Prozess der Einführung der Bodycams ist erfolgt und wird fortgesetzt.

Section Control

(TB, Seiten 39 bis 40)

Die Stellungnahme der Landesregierung zum XXII. Bericht über die Tätigkeit der LfD für die Jahre 2013 und 2014 (Drs 17/5855) beinhaltet bereits einen umfangreichen Bericht zum beabsichtigten Pilotprojekt zur Geschwindigkeitsabschnittsüberwachung „Section Control".

Zur Aktualisierung dessen und zur thematischen Darstellung im 23. Tätigkeitsbericht sind folgende Ergänzungen zum aktuellen Stand hinzuzufügen, die in der zeitliche Folge eingetreten sind:
Im Anschluss an den dargestellten Berichtszeitraum 2015 bis 2016 hat die Polizeidirektion Hannover im Dezember 2017 gegenüber der LfD bezüglich deren Anmerkungen im Schreiben vom 17.05.2016 umfassend schriftlich berichtet. Nach dessen Prüfung hat die LfD der Polizeidirektion Hannover im März 2018 mitgeteilt, dass sie der Argumentation grundsätzlich folgt. Dazu stellt die LfD noch einmal heraus, dass vor dem Start des Pilotbetriebes

- eine angepasste, die aktuellen Diskussionsstände, Prüfungen, Abwägungen und Erkenntnisse umfassende, nachvollziehbare und fortschreibungsfähige Vorabkontrolle erstellt sein wird und
- die Zulassung der Physikalisch-Technischen Bundesanstalt (PTB) vorliegt.

Des Weiteren erwartet sie, dass vor dem „Echtbetrieb“ eine gesetzliche Grundlage für diese besondere Art der Geschwindigkeitsüberwachung in Niedersachsen geschaffen wird.

Die Anpassung der Vorabkontrolle ist, soweit erforderlich, von der Polizeidirektion Hannover gewährleistet worden. Die PTB erteilte am 06.11.2018 die Baumusterprüfbescheinigung für die Pilotanlage. Nach anschließender Eichung erfolgte am 19.12.2018 die Inbetriebnahme der Anlage, zunächst nur zum Zwecke des Tests des ganzheitlichen Verfahrensablaufes von der Feststellung des Geschwindigkeitsverstoßes bis zur Auswertung und Sachbearbeitung bei der zuständigen Bußgeldbehörde. Nach dessen erfolgreichem Verlauf startete am 14.01.2019 der Pilotbetrieb über maximal 18 Monate. Die Beendigung ist spätestens zum 30.06.2020 vorgesehen. Der Gesetzentwurf der Landesregierung zur Änderung des Nds. SOG setzt die Forderung bezüglich der Schaffung einer Rechtsgrundlage um.

Datenverarbeitung der Polizei bei Teilnahme an einer friedlichen Versammlung
(TB, Seiten 41 bis 43)
Die LfD erörtert zu diesem Thema die Frage der Rechtmäßigkeit der Speicherung und Löschung personenbezogener Daten bei friedlich verlaufenen Versammlungen. Sie verweist auf die Ergebnisse einer bei den Polizeidirektionen veranlassten Überprüfung und kritisiert die PD Lüneburg, die der Aufforderung der LfD nach Löschung der betreffenden Datensätze nicht in vollem Umfang nachkam.

Die Rechtsauffassung der LfD, dass personenbezogene Daten von friedlichen Versammlungsteilnehmerinnen und Versammlungsteilnehmern bei völlig störungsfreien Versammlungen grundsätzlich nicht zu speichern sind, wird von der Landesregierung geteilt. Bereits mit

Erlass vom 11.05.2012 waren die niedersächsischen Polizeidirektionen, das LKA und die Zentrale Polizeidirektion darauf hingewiesen worden, dass die Speicherung personenbezogener Daten von Versammlungsleiterinnen und Versammlungsleitern in Fällen störungsfrei verlaufener Versammlungen in der Regel nicht erforderlich sein dürfte.

Das Ergebnis der oben angegebenen Überprüfung der LfD wurde zum Anlass genommen, die Polizeidirektionen, das LKA, die ZPD und die Polizeiakademie Niedersachsen zu bitten, bei der Speicherung von personenbezogenen Daten im Zusammenhang mit Versammlungen besonders sensibel zu agieren und ihre Vorgehensweise entsprechend zu überprüfen. Sie wurden darauf hingewiesen, dass für eine Speicherung von personenbezogenen Daten in den jeweiligen Einzelfällen hinreichende Gründe, etwa nach § 38 Abs. 1 Nds. SOG, vorliegen müssten. In Fällen, in denen Versammlungen störungsfrei verlaufen sind, dürfte eine Speicherung in der Regel nicht erforderlich sein.

Mangelhafte Auskunft bei der Polizei

(TB, Seiten 46 bis 47)

Gegenüber dem Ministerium für Inneres und Sport wurde im Dezember 2016 durch die LfD eine förmliche Beanstandung aufgrund einer unvollständigen Auskunftserteilung im Rahmen eines ersten Auskunftsersuchens sowie der Löschung gespeicherter Daten in „SAFIR“ während eines laufenden zweiten Auskunftsersuchens ausgesprochen. In der hierzu im März 2017 erfolgten Stellungnahme an die LfD wurde bereits ausgeführt, dass das zu Grunde gelegte datenschutzrechtliche Verhalten im Ergebnis der Überprüfung aus verschiedenen Gründen heraus von hier weder einschlägig bestätigt noch widerlegt werden konnte.

Im Rahmen der Aufgabenbewältigung der Polizei Niedersachsen werden Abläufe und Verfahren hinsichtlich etwaiger Anpassungs- bzw. Optimierungsbedarfe geprüft. Im April 2018 wurden z. B. durch die behördlichen Datenschutzbeauftragten der Polizeibehörden die Verfahrensabläufe bei Auskunftserteilungen harmonisiert und ein grundsätzliches Bearbeitungsmuster abgestimmt.

Prüfung einer nicht-individualisierten Funkzellenabfrage

(TB, Seiten 48 bis 51)

Die LfD unterstützt in ihrem Bericht die Einführung einer aussagekräftigen Statistik zu Funkzellenabfragen.

Eine detaillierte Statistik über Funkzellenabfragen wäre aus Sicht der Landesregierung mit einem hohen Verwaltungsaufwand für die Strafverfolgungsbehörden bei unklarem Nutzen einer entsprechenden Statistik verbunden.

Mit Wirkung zum 24.08.2017 hat der Bundesgesetzgeber in § 101b Abs. 5 Strafprozessordnung (StPO) eine Berichtspflicht für die Länder und den Generalbundesanwalt zu angeordneten Maßnahmen nach § 100g StPO geschaffen. Die Länder und der Generalbundesanwalt haben dem Bundesamt für Justiz jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100g StPO zu berichten. Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet. Durch die Veröffentlichung soll die Transparenz der Maßnahmen gestärkt und ihre Evaluierung erleichtert werden. Die Übersichten nach § 101 b StPO sind erstmalig für das Berichtsjahr 2019 zu erstellen (vgl. hierzu die Übergangsregelung in § 16 Einführungsgesetz StPO).

Ordnungswidrigkeiten-Verfahren bei Datenschutzverstößen

(TB, Seiten 54 bis 56)

Die LfD stellt das Ergebnis ihrer im Berichtszeitraum durchgeführten Erhebung zu Ordnungswidrigkeiten-Verfahren nach Datenschutzverstößen im kommunalen Bereich vor. Sie stellt insgesamt fest, dass die Anzahl der Verfahren in der Landesverwaltung und den Kommunen aus ihrer Sicht zu gering sei.

Eine Ordnungswidrigkeit nach § 29 NDSG a.F. lag u.a. vor, wenn Beschäftigte öffentlicher Stellen personenbezogene Daten unrechtmäßig im Sinne des § 29 Absatz 1 Nr. 1 NDSG a.F. verarbeitet haben.

Die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten bei Zuwiderhandlungen gemäß § 29 NDSG a.F. waren im Berichtszeitraum in § 7 Nr. 12 der Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten (ZustVO-OWi) geregelt. Zuständig war bei derartigen Verstößen durch Beschäftigte der Daten verarbeitenden Stelle die jeweilige Aufsichtsbehörde bzw. die Daten verarbeitende Stelle selbst, wenn sie als oberste Landesbehörde einer behördlichen Aufsicht nicht untersteht oder wenn ihre unmittelbare Aufsichtsbehörde eine oberste Landesbehörde ist. Aufsichtsbehörde im Sinne dieser Regelung ist die jeweilige Rechtsaufsichtsbehörde und nicht die LfD. Der Landesregierung liegen keine Zahlen zu Datenschutzverstößen im Sinne des § 29 NDSG a.F. vor. Die Landesregierung geht davon aus, dass die Rechtslage bekannt ist und die jeweiligen Behörden diese beachten. Im Übrigen müssen Ordnungswidrigkeiten-Verfahren nicht regelmäßig zur Verhängung von Geldbußen führen; nach § 47 Abs. 1 des Gesetzes über Ordnungswidrigkeiten haben die Bußgeldbehörden hier ein Ermessen (sog. Opportunitätsprinzip).

Mit Bezug auf die DSGVO fordert die LfD die Ausweitung der Sanktionsregelungen für den

öffentlichen Bereich und die Schaffung einer Möglichkeit, auch gegen Behörden – wie bei nicht öffentlichen Stellen – Geldbußen bei datenschutzrechtlichen Verstößen verhängen zu können.
Dieser Forderung der LfD, die diese bereits im Rahmen der Verbandsanhörung zum Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts vorgebracht hatte, ist die Landesregierung nicht gefolgt. Alle öffentlichen Stellen sind an Recht und Gesetz gebunden; die Verhängung einer Geldbuße durch eine öffentliche Stelle gegenüber einer anderen öffentlichen Stelle wird als systemfremd gesehen.
Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, darf die LfD gemäß § 20 Absatz 5 NDSG in der Fassung ab 25.05.2018 Geldbußen gegen diese verhängen. Damit soll sichergestellt werden, dass öffentliche Stellen, die im Rahmen ihrer Tätigkeit im Wettbewerb mit anderen Verarbeiterinnen und Verarbeitern stehen, gegenüber ihren Mitbewerberinnen und Mitbewerbern nicht bessergestellt werden.

„Deutschland-Cloud“

(TB, Seiten 57 bis 59)

Die LfD schildert in ihrem Bericht die Prüfung der Umsetzung der Testumgebung zur Referenzumgebung II in diesem Modell. Die LfD ist seitens des Justizministeriums von Beginn bis zum Abschluss in die Prüfung einbezogen worden. Der im Bericht dargestellte Sachverhalt entspricht den Prüfungsergebnissen. Die Firma Microsoft hat das Geschäftsmodell „Deutschland-Cloud“ zwischenzeitlich eingestellt.

Datenschutzrechtliche Aspekte des „Financial Blocking“ nach dem Glücksspielstaatsvertrag

(TB, Seiten 60 bis 61)

Die Einschätzung der LfD, dass Maßnahmen zur Zahlungsunterbindung im Zusammenhang mit unerlaubtem Glücksspiel für datenschutzrechtlich bedenklich gehalten werden, wird von der Landesregierung nicht geteilt.

Es kann dahinstehen, ob der Glücksspielstaatsvertrag (GlüStV) eine Rechtsgrundlage zur umfassenden Datenverarbeitung vorsieht, da personenbezogene Daten von Kundinnen und Kunden der betroffenen Zahlungsanbieter seitens des Ministeriums für Inneres und Sport weder erhoben noch verarbeitet werden.
Bei der Einleitung von Maßnahmen zur Zahlungsunterbindung verfolgt das Ministerium für Inneres und Sport vorrangig einen kooperativen Ansatz. Die betroffenen Zahlungsanbieter sollen danach vorzugsweise im Rahmen ihrer eigenen Geschäftspolitik („compliance“) sicherstellen, dass ihr Zahlungsmittel nicht für unerlaubtes und bereits untersagtes Glücksspiel

zur Verfügung steht. Die betroffenen Unternehmen sollen anknüpfend an ihre eigene gesetzliche Verpflichtung rechtskonformen Verhaltens die Geschäftsbeziehung zu rechtswidrigen Glücksspielanbietern insgesamt überprüfen und ggfls. beenden bzw. darauf einwirken, dass illegale und legale Zahlungsströme voneinander zu trennen sind. Schließlich enthält § 4 Abs. 1 Satz 2 GlüStV bereits ein allgemeines Verbot, an Zahlungen im Zusammenhang mit unerlaubtem Glücksspiel mitzuwirken, das sich an die am Zahlungsverkehr Beteiligten richtet. Die Zahlungsanbieter sind also bereits selbst und unmittelbar verpflichtet.
Auch eine umfassende Speicherung von Daten über den Zahlungsverkehr zu Überprüfungszwecken der Glücksspielaufsicht ist nicht geplant.

Dass nach Ansicht der LfD die Zahlungsunterbindung nicht die Auszahlung des Gewinns von der Bank an die Spielerin oder den Spieler erfassen solle, da dies eine unzulässige Lokalisation bedeuten würde, kann ebenfalls nicht bestätigt werden. Es kommt allein darauf an, ob es sich um Zahlungen im Zusammenhang mit unerlaubtem Glücksspiel handelt.

Es liegt in der Eigenverantwortung der Zahlungsanbieter, in welcher Form sie dem gesetzlichen Mitwirkungsverbot nachkommen. Entscheidend ist allein, dass eine Mitwirkung an Zahlungen in Zusammenhang mit unerlaubtem Glücksspiel unterbleibt. Es ist davon auszugehen, dass die Zahlungsanbieter, etwa aufgrund der bestehenden vertraglichen Beziehungen, über die notwendigen Möglichkeiten verfügen, die erforderlichen Maßnahmen einzuleiten. Dass gegebenenfalls auch deutsche Spielerinnen und Spieler, die kurzeitig im Ausland (legal) spielen, von Sperrungen ihres gewohnten Zahlungsanbieters erfasst würden, oder auch Zahlungen, die rechtmäßige Angebote desselben Anbieters betreffen, auf diesem Wege verhindert würden, wäre in diesem Fall notwendige und unvermeidbare Folge. Anbietern steht es insoweit frei, legale und illegale Zahlungsströme entsprechend der gesetzlichen Vorgaben voneinander zu trennen. Eine andere Bewertung würde stets dazu führen, dass derjenige, der neben seinem rechtswidrigen Angebot auch einen (wenn auch nur kleinen) legalen Teil anbietet, nicht belangt werden könnte. Dies ließe sich nicht mit der Rechtsstaatlichkeit vereinbaren.
Hinzuweisen ist auch darauf, dass die Veranstaltung von und die Beteiligung an unerlaubtem Glückspiel nach Maßgabe der §§ 284 und 285 StGB strafbar sind.

Richtlinie zur Förderung der politischen Jugendbildung
(TB, Seite 63)
Die Richtlinie des Ministeriums für Soziales, Gesundheit und Gleichstellung vom 07.12.2015 über die Gewährung von Zuwendungen zur Förderung der politischen Jugendbildung wurde

von der LfD datenschutzrechtlich überprüft. Dabei bemängelte die LfD, dass die gewählte Formulierung in der Richtlinie nicht gewährleisten könne, dass keine Rückschlüsse auf die politische Ausrichtung einzelner Teilnehmerinnen und Teilnehmer der geförderten Maßnahme gezogen werden können.
Die Richtlinie wurde inzwischen den Hinweisen der LfD entsprechend geändert.

Übermittlung von Flüchtlingsdaten durch öffentliche Stellen
(TB, Seite 64 bis 65)
Die LfD hat sich im Berichtszeitraum mit der Überprüfung der Zulässigkeit von Datenübermittlungen von Flüchtlingsdaten im Zusammenhang mit deren Erstaufnahme befasst.
Bei der Erstaufnahme und Unterbringung von Flüchtlingen in Niedersachsen erfolgte in den Jahren 2015/2016 vielfach die Erhebung von personenbezogenen Daten durch private Hilfsorganisationen wie das Deutsche Rote Kreuz (DRK) oder die Johanniter Unfallhilfe (JUH). Die erhobenen Daten wurden u.a. zum Zweck der Essensversorgung genutzt, aber auch zur weiteren Nutzung für Leistungen der Landesaufnahmebehörde Niedersachsen (LAB NI) an diese weitergeleitet. Hierbei handelte es sich um eine Auftragsdatenverarbeitung gem. § 6 NDSG a.F., die den Abschluss entsprechender Auftragsdatenverarbeitungsverträge zwischen der LAB NI und den jeweiligen Beauftragten erforderte.

Für die im Zeitraum vom 05.10.2015 – 22.09.2016 vom DRK im Auftrag des Landes betriebene Notunterkunft im Camp Fallingbostel-Ost wurde damals kein Vertrag über die Datenverarbeitung geschlossen. Eine nachträgliche Legitimierung der erfolgten Datenverarbeitung durch Abschluss einer entsprechenden Vereinbarung kommt aus rechtlichen Gründen nicht in Betracht.

Bei künftigen bzw. laufenden vergleichbaren Fällen der Beauftragung von Hilfsorganisationen oder Unternehmen mit der Auftragsverarbeitung gem. Art. 28 i.V.m. Art. 4 Nr. 8 DSGVO im Geschäftsbereich der LAB NI wird darauf geachtet, dass von der LAB NI entsprechende schriftliche Vereinbarungen abgeschlossen werden.

Anforderungen durch das neue Bundesmeldegesetz
(TB, Seiten 66 bis 68)
Die LfD erläutert die Rechtslage zu verschiedenen Fallgestaltungen bezüglich des neuen Melderechts.
Mit dem am 01.11.2015 in Kraft getretenen Bundesmeldegesetz (BMG) wurden sowohl die bis dahin geltenden Meldegesetze der Länder – mithin auch das Niedersächsische Meldegesetz – als auch das Melderechtsrahmengesetz des Bundes abgelöst.

Als Hilfestellung zur Auslegung und Anwendung der einzelnen Vorschriften hat die Bundesregierung die „Allgemeine Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes vom 28. Oktober 2015“ (BMGVwV) erlassen. Zum anderen hat das Niedersächsische Ministerium für Inneres und Sport in den vergangenen Jahren verschiedene Erlasse an die Kommunen herausgegeben, um diese bei der Anwendung einzelner Vorschriften des BMG zu unterstützen.

Die von der LfD geschilderten Einzelfälle konnten nach Rücksprache ohne weitergehendes fachaufsichtliches Einschreiten geklärt werden.

Hinsichtlich der Übermittlung von Meldedaten zum Zwecke der Wahlwerbung ist zu ergänzen, dass es sich bei den übermittelten Daten gem. § 50 Abs. 1 i.V.m. § 44 Abs. 1 Satz 1 BMG um den Familiennamen, frühere Namen, Vornamen unter Kennzeichnung des gebräuchlichen Vornamens, Doktorgrad, derzeitige Anschriften und, sofern die Person verstorben ist, diese Tatsache, handelt. Diese Melderegisterauskunft erfolgt durch eine Datenübermittlung, nicht durch eine Datenweitergabe (eine solche erfolgt gem. § 37 Abs. 1 BMG nur innerhalb der jeweiligen Verwaltungseinheit). Die Pflicht der Meldebehörden, auf die diesbezüglich bestehende Widerspruchsmöglichkeit bei Anmeldung nach § 17 Abs. 1 BMG sowie einmal jährlich durch öffentliche Bekanntmachung hinzuweisen, folgt aus § 50 Abs. 5 BMG.

Beratende Funktion im Nds. IT-Planungsrat
Ende-zu-Ende-Verschlüsselung
(TB, Seite 70)
Die LfD knüpft an ihren vorigen Tätigkeitsbericht an und fordert, dass „Daten ab der Schutzstufe D (…) nur Ende-zu-Ende-verschlüsselt übertragen werden, weil regelmäßig wiederkehrend (wenngleich auch mit geringem Anteil) durch Bedienfehler oder mangelnde Achtsamkeit Daten an falsche Empfängerinnen und Empfänger versandt werden…“.
Bereits seit Jahren werden E-Mails innerhalb des Landesnetzes zwischen den E-Mail-Servern einerseits und zwischen E-Mail-Servern und den Arbeitsplatzcomputern anderseits verschlüsselt übertragen und dadurch vor der Einsichtnahme unbefugter Dritter geschützt. Eine Ende-zu-Ende-Verschlüsselung in dem Sinne, dass nur die Senderin oder der Sender und die Empfängerin oder der Empfänger die E-Mail lesen können, erfolgt hingegen nicht.

Die E-Mails werden auf den E-Mailservern unverschlüsselt abgelegt. Die Landesregierung hat bereits in der Stellungnahme zum XXII. Bericht über die Tätigkeit der LfD ausgeführt, dass eine Ende-zu-Ende-Verschlüsselung zu zahlreichen Problemen führt, die bisher nicht gelöst sind. Die LfD führt in ihrem Tätigkeitsbericht zudem selbst aus, dass „die Einführung

einer wirksamen Ende-zu-Ende-Verschlüsselung den Einsatz „von Virenscannern auf Firewalls ebenso aushebeln würde, wie auch das zentrale Scannen auf dem Mailserver“. D.h., dass einem eventuellen Gewinn an Vertraulichkeit ein Verlust an Sicherheit an anderer Stelle entgegenstehen würde.
Eine Ende-zu-Ende-Verschlüsselung wäre insbesondere auch nicht geeignet, das Problem der falschen Adressierung zu lösen. Wer die richtige Empfängerin oder der richtige Empfänger einer Nachricht ist, ist eine organisatorische Frage. Wählt eine Beschäftigte oder ein Beschäftigter eine Empfängerin oder einen Empfänger aus, würde eine Verschlüsselung nur gewährleisten, dass ausschließlich die ausgewählte Empfängerin oder der ausgewählte Empfänger die E-Mail entschlüsseln kann. Es besteht immer das Risiko, dass der Beschäftigten oder dem Beschäftigten bei der Auswahl ein Fehler unterläuft.

Niedersachsen-Client

Virenscanner

(TB, Seiten 71 bis 72)

Die LfD führt aus, dass Virenscanner nur von beschränktem Nutzen für die IT-Sicherheit sind. Unter Verweis auf unterschiedliche Online-Quellen[1] sieht sie das Konzept des Virenscanners in Frage gestellt.
Die Landesregierung teilt die Einschätzung, dass Antiviren-Software keinen absoluten Schutz vor Schadsoftware bieten. Vielmehr sind sie nur eine Komponente, um den Gefahren, die von Schadsoftware ausgehen, zu begegnen. So führt das Bundesamt für Sicherheit in der Informationstechnologie (BSI) im Baustein 1.6 der IT-Grundschutzkataloge aus: „Die wichtigsten vorbeugenden Maßnahmen gegen Schäden durch Schadsoftware sind der Einsatz von Viren-Schutzprogrammen sowie regelmäßige Datensicherungen.“ Die Landesregierung erkennt keine allgemeine Diskussion in der Fachöffentlichkeit dahingehend, dass Antiviren-Software verzichtbar sein könnte. Aus den von der LfD referenzierten Quellen ergibt sich nichts anderes:

- Der von heise.de zitierte Experte verweist zwar auf Schwächen von bestimmten Produkten und empfiehlt deren De-Installation[2], macht aber eine Ausnahme für die Software, die das Land auf dem NiedersachsenClient und dem PolizeiClient einsetzt.
- Die Landesregierung versteht die bei heise.de zitierten Äußerungen des Vizepräsidenten eines Unternehmens aus der IT-Sicherheitsbranche nicht dahingehend, dass er Antiviren-Software für überflüssig hält. Vielmehr ergibt sich für das im Beitrag erwähnte Unternehmen Handlungsbedarf dadurch, dass derartige Software heute re-

[1] Insbesondere https://www.heise.de/security/artikel/Ex-Firefox-Entwickler-raet-zur-De-Installation-von-AV-Software-3609009.html und https://www.heise.de/security/meldung/Symantec-erklaert-Antivirus-Software-fuer-tot-2183311.html
[2] https://robert.ocallahan.org/2017/01/disable-your-antivirus-software-except.html

gelmäßig im Betriebssystem enthalten ist und es Drittanbietern damit schwerer fällt, ihre Produkte zu verkaufen.

Ransomware

(TB, Seite 72)

Der Tätigkeitsbericht führt aus, dass auch Landesbehörden Opfer von Angriffen mit Ransomware, also Software, die die Datenbestände der angegriffenen Institution verschlüsseln, waren.

Aus Sicht der Landesregierung unterstreicht das Beispiel „Ransomware“ den Bedarf, Schadprogramme mit Software abzuwehren. So gelingt es jedenfalls, Angriffe, die mit bekannter Schadsoftware durchgeführt werden, abzuwehren. Dem Computer-Notfallteam Niedersachsen (NCert) ist kein Fall bekannt, in dem ein Angriff mit Ransomware gegen Infrastruktur der unmittelbaren Landesverwaltung erfolgreich war.

Sicherheitsdomänen u. Virtualisierung

(TB, Seiten 72 bis 73)

Die LfD sieht einen Bedarf für eine Virtualisierung von Webbrowser und Mailclient und fordert Abschottungsmaßnahmen der Netzsegmente untereinander.

Aus Sicht der Landesregierung besteht kein unmittelbarer Zusammenhang zwischen diesen Einzelmaßnahmen. Die Nutzung eines Webbrowsers in einer virtualisierten Umgebung dient dazu, den Befall mit Schadprogrammen unwahrscheinlicher zu machen. Die Abschottung von Netzsegmenten kann dazu beitragen, den Schaden, der durch einen Befall mit Schadprogrammen entsteht, zu begrenzen.

Wird ein Webbrowser in einer virtualisierten Umgebung genutzt, kann damit der Schutz vor Gefahren, die von außen auf die Infrastruktur des Landes einwirken, unter Umständen über das ohnehin schon bestehende Schutzniveau hinaus weiter verbessert werden. In den strengen Mindeststandards, die das BSI gem. § 8 Abs. 1 BSI-Gesetz für die Informationstechnik des Bundes festlegt, wird eine Virtualisierung des Webbrowsers nicht gefordert.

Die Landesregierung legt neben dem bestmöglichen Schutz der Daten Wert darauf, dass die Arbeitsfähigkeit der Verwaltung erhalten bleibt. Der Landesbetrieb IT.Niedersachsen hat eine Machbarkeitsstudie bzgl. der Virtualisierung des Webbrowsers durchgeführt. Dabei zeigten sich noch erhebliche Schwächen des getesteten Produkts. So erfordert die Lösung beispielsweise eine Schulung der Anwenderinnen und Anwender, weil Standardfunktionen wie Drucken und Speichern nicht wie gewohnt funktionieren. Der Aufruf der Anwendung dauerte bis zu 30 Sekunden und Videos ließen sich nicht störungsfrei abspielen. Der Landesbetrieb wird den Markt für Virtualisierungsprodukte jedoch weiter beobachten.

Die Forderung nach „Abschottungsmaßnahmen der Netzsegmente untereinander“ kann die Landesregierung nicht nachvollziehen, da es bereits abgeschottete Netzsegmente (z.B. für die Polizei) gibt.

Polizeiclient

(TB, Seite 73)

Die LfD stellt „die zunehmende technische Monokultur in der Landesverwaltung durch Umstellung der Polizeiarbeitsplätze von Linux auf eine Variante des Niedersachsenclients“ als Risiko dar.

Die Landesregierung ist nicht der Ansicht, dass der Einsatz unterschiedlicher Betriebssysteme Vorteile bietet, die die Vorteile einer standardisierten Lösung übertreffen. Sie sieht vor allem die Gefahr, dass die Ressourcen der Landesverwaltung langfristig nicht ausreichen, um mehrere Systeme parallel sicher zu betreiben. Für die Sicherheit der Daten der Bürgerinnen und Bürger, die auf IT-Systemen des Landes verarbeitet werden, ist nach Auffassung der Landesregierung nicht das Betriebssystem allein entscheidend. Vielmehr kommt es auf das Zusammenwirken unterschiedlicher Maßnahmen (z.B. Firewalls, Virenschutz, Updates, Verschlüsselung, Datensicherung usw.) an. Die Landesregierung ist bestrebt, die für die Gewährleistung und stetige Verbesserung der Sicherheitsmaßnahmen erforderliche Kompetenz zu bündeln, da sie sich hiervon eine besonders hohe Arbeitsqualität verspricht. Gerade bei der Modernisierung der Polizei-IT hat sich diese Strategie bewährt:

So wurde z.B. eine „Enhanced Security Administrative Environment (ESAE) Architecture“ aufgebaut, um IT-Komponenten in „Ebenen“ zu segmentieren. Diese Maßnahme stellt eine hochmoderne und zukunftsfähige Grundlage dar, stetig wachsenden Bedrohungen aus dem Cyberraum auch im Sinne der bei der Etablierung von Informationssicherheitsmaßnahmen zu beachtenden Wirtschaftlichkeit und einem hieraus resultierenden angemessenen Informationssicherheitsniveau wirksam zu begegnen.

Schulen

Einsatz von Tablets im Schulunterricht

(TB, Seite 79)

Das niedersächsische Landesinstitut für schulische Qualitätsentwicklung hatte lt. Bericht der LfD im Jahr 2016 den Entwurf eines Leitfadens zum Einsatz mobiler Computer im Unterricht vorgelegt. Dieser wurde in datenschutzrechtlicher Hinsicht zusammen mit der LfD erörtert.

Trotz zahlreicher Abstimmungsversuche bestehen zum Leitfaden in einer Reihe von Punkten unterschiedliche Rechtsauffassungen zwischen dem Kultusministerium und der LfD. Inzwischen hat die LfD mitgeteilt, dass aufgrund der verschiedenen Rechtspositionen Hinweise

nicht mehr für zielführend angesehen werden und sie zu dieser Thematik eigene Informationen auf ihrer Homepage einstellen wird.

Einsatz privater IT-Systeme zur Erledigung dienstlicher Aufgaben

(TB, Seite 80)

Das Kultusministerium hat mit Runderlass vom 01.02.2012 „Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Lehrkräften“ geregelt, unter welchen Voraussetzungen die Lehrkräfte ihre eigenen, privaten IT-Geräte einsetzen dürfen. Der Erlass ist nach Rechtsauffassung der LfD bezüglich des Einsatzes mobiler Endgeräte einzuschränken.

Der Runderlass wird unter Einbeziehung der Sicherheitsbedenken der LfD hinsichtlich der Verwendung mobiler Endgeräte neu erlassen. Das Anhörungsverfahren der hiervon berührten Verbände wurde durchgeführt.

Foto- und Filmaufnahmen in der Schule

(TB, Seite 81)

In dem Bericht erläutert die LfD die Rechtslage und die Voraussetzungen für das zulässige Anfertigen von Fotos und Filmaufnahmen von Schülerinnen und Schülern.

Die Landesregierung teilt die Rechtsauffassung der LfD. Das Kultusministerium und die Landesschulbehörde (NLSchB) beraten die Schulen entsprechend.

Datenschutzbeauftragte

Datenschutzbeauftragte in Schulen

(TB, Seiten 100 bis 101)

In LfD hat stichprobenartig niedersächsische Schulen hinsichtlich der Bestellung von Datenschutzbeauftragten überprüft und festgestellt, dass fast die Hälfte davon noch keine Datenschutzbeauftragten bestellt hat.

Dieses Ergebnis wurde durch das Kultusministerium in einer Umfrage im Jahr 2016 bestätigt. Defizite bestehen vor allem bei kleinen allgemeinbildenden Schulen. Um diese bei der Bestellung von Datenschutzbeauftragten zu unterstützen, findet ein regelmäßiger Informationsaustausch der Schulen mit den Dezernentinnen und Dezernenten für Datenschutz bei der NLSchB statt.

Im Zeitraum seit dem 01.04.2018 wurde der NLSchB die Neubestellung von Datenschutzbeauftragten an gut 200 öffentlichen Schulen gemeldet. Die Dezernentinnen und Dezernenten für Datenschutz bei der NLSchB arbeiten intensiv daran, dass die Zahl der Neubestellungen von Datenschutzbeauftragten weiter steigt.

Bestellung einer juristischen Person zum Datenschutzbeauftragten

(TB, Seiten 102 bis 103)

Die LfD erläutert ihre Rechtsauffassung zu der Frage, ob eine Rechtsanwalts-Partnerschaftsgesellschaft im Sinne des Partnerschaftsgesellschaftsgesetzes (PartGG) als externer betrieblicher Datenschutzbeauftragter bestellt werden kann.

Wenn die LfD bei ihrer Prüfung – nach alter Rechtslage – unter Verweis auf §§ 4f und 4g BDSG in der bis zum 24.05.2018 geltenden Fassung bzw. auf das PartGG zu dem Ergebnis kommt, dass eine Rechtsanwalts-Partnerschaftsgesellschaft nicht als externe betriebliche Datenschutzbeauftragte bestellt werden könne, da nur natürliche Personen hierzu in der Lage seien, ist dazu aus justizfachlicher Sicht nichts anzumerken.

Soweit die LfD in ihrem Tätigkeitsbericht darauf hinweist, dass sich an dem Ergebnis ihrer Prüfung auch nach dem Inkrafttreten der DSGVO voraussichtlich nichts ändern werde, ist hierzu Folgendes zu bemerken:

Erwägungsgrund 97 DSGVO stützt ihre Auffassung, insoweit dort von „einer weiteren Person“ die Rede ist, „die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt […]“. Nach Art. 37 Abs. 5 DSGVO werden Datenschutzbeauftragte auf Grundlage ihrer beruflichen Qualifikation und ihres Fachwissens benannt. Nur natürliche Personen können die nötige „berufliche“ Fachkunde und Zuverlässigkeit aufweisen und nur zu diesen ist eine vertrauliche Beziehung der Beteiligten möglich (so auch Bergt, in: Kühling/Buchner, DSGVO - BDSG, 2. Aufl. 2018, Art. 37 Rn. 33 ff.).

Die sog. Artikel-29-Gruppe (nunmehr: EU-Datenschutzausschuss) hält hingegen zumindest in ihrer unverbindlichen Auslegungshilfe („Working Paper 243“ vom 16.12.2016, überarbeitet am 05.04.2017) die Benennung einer juristischen Person zum externen Datenschutzbeauftragten für möglich. Voraussetzung hierfür sei jedoch, dass „jedes Mitglied der Einrichtung, das die Funktion eines Datenschutzbeauftragten wahrnimmt“, sämtliche der in Abschnitt 4 der DSGVO (Datenschutzbeauftragter) genannten Anforderungen erfülle (s. https://www.ldi.nrw.de/DE-wp243rev01.pdf, S. 14). Dies dürfte die Benennung einer juristischen Person als Datenschutzbeauftragte schon per se zumindest unattraktiv machen.

Soweit die LfD abschließend ausführt, sie werde künftig auch nur die Benennung von natürlichen Personen zu (betrieblichen) Datenschutzbeauftragten akzeptieren, kann zur Benennung einer juristischen Person in der Praxis jedenfalls nicht geraten werden.

Datenschutz in der Wirtschaft

Was Immobilienmakler alles wissen wollen

(TB, Seiten 112 bis 114)

Im Rahmen einer anlassfreien Prüfung hat die LfD sich mit der Frage befasst, was Vermieterinnen und Vermieter zu welchem Zeitpunkt im Vermietungsprozess fragen dürfen. Da im Berichtszeitraum ein Verbot des Scannens, Fotografierens und Ablichtens des Personalausweises bestand, wurde u.a. die Anfertigung von Ausweiskopien beanstandet.
Dieses Verbot wurde mit dem Gesetz zur Förderung des elektronischen Identitätsnachweises, welches am 15.07.2017 in Kraft trat, als nicht praxisgerecht erachtet. § 20 Abs. 2 Personalausweisgesetz (PAuswG) hat nunmehr folgende Fassung:
„(2) [1]Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. [2]Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. [3]Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. [4]Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.“

Im behördlichen wie auch im privaten Bereich kann demnach ein berechtigtes Bedürfnis für das Kopieren des Personalausweises bestehen, welchem durch den neuen § 20 Abs. 2 PAuswG Rechnung getragen wurde. Aufgrund der allgemeinen Handlungsfreiheit obliegt der Ausweisinhaberin oder dem Ausweisinhaber grundsätzlich die Entscheidung darüber, ob eine Ablichtung (Fotokopie, Fotografie, Scan) ihres bzw. seines Ausweises erfolgen soll. Gleichzeitig wird das öffentliche Interesse an dem Personalausweis als Identifizierungsdokument dadurch gewahrt, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar sein muss.

Beschäftigtendatenschutz

E-Mail und Internet am Arbeitsplatz

(TB, Seiten 138 bis 140)
Die LfD erläutert die wesentlichen Eckpunkte der Orientierungshilfe, die von den Datenschutzaufsichtsbehörden zum Thema datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz erstellt wurde.
Je nach Dienstanweisung und Vorgaben zur Nutzung durch den jeweiligen Dienstherrn ergeben sich die Folgen für die Beschäftigten und die datenschutzrechtlichen Befugnisse des Dienstherrn.
In der Landesverwaltung wird die datenschutzgerechte Nutzung dieser Dienste in der Regel durch Dienstanweisungen vorgegeben. Einige Beispiele sind im Folgenden dargestellt:
Im **Ministerium für Wissenschaft und Kultur** war im Berichtszeitraum für die Bediensteten die Dienstanweisung für die Nutzung der IT-Ausstattung vom 01.08.2012 wirksam. Dort

wurde geregelt, dass Internetdienste, der E-Mail-Dienst sowie die IT-Arbeitsplatzausstattung der Beschäftigten als Arbeitsmittel nur im Rahmen ihrer Aufgabenerfüllung zur Verfügung standen. Im Rahmen der „betrieblichen Übung“ hat die Behördenleitung die private Nutzung in geringem Umfang jedoch geduldet, was allgemein als konkludente Genehmigung angesehen wird.
Seit dem 20.03.2018 besteht die Dienstanweisung über die private Nutzung von dienstlichen IT-Systemen zwischen dem Ministerium für Wissenschaft und Kultur und dem Personalrat des Ministeriums für Wissenschaft und Kultur. Diese ist auf der Grundlage der Informationssicherheitsrichtlinie über die Nutzung von Informationstechnik durch Anwenderinnen und Anwender (ISRL-IT-Nutzung, Gem. RdErl. d. MI, d. StK u.d.übr. Min. v. 9.11.2016 (Nds. MBl. S. 1193) erstellt worden. Insofern sind mit dieser Dienstanweisung bereits die Orientierungshilfen, die im Tätigkeitsbericht der LfD angeführt werden, umgesetzt.

In der **niedersächsischen Justiz** ist die Nutzung von E-Mail und Internet am Arbeitsplatz in mehreren Dienstvereinbarungen gemäß § 78 NPersVG zwischen dem Justizministerium und den Stufenvertretungen mit Wirkung für den gesamten Geschäftsbereich wie folgt geregelt:
Internet:
In der Dienstvereinbarung „… über die private Nutzung dienstlicher IT-Systeme einschließlich des dienstlichen Internet-Zugangs und des dienstlichen E-Maildienstes“ wird die Erlaubnis einer privaten Nutzung des Internet-Zugangs in einem angemessenen Umfang gewährt. Zudem werden in dieser Dienstvereinbarung die einzuhaltenden Rahmenbedingungen, sowie die Protokollierung – auch privat motivierter – Internet-Zugriffe geregelt.
In der Dienstvereinbarung „… über die Kontrolle der Internetnutzung“ sind der Umfang und die Rahmenbedingungen der Kontrolle der Internetnutzung vereinbart. Im Wesentlichen werden die Protokolle auf Behördenebene gefiltert und dem Disziplinarvorgesetzten anonymisiert zur stichprobenartigen Kontrolle zur Verfügung gestellt. Nur in einem konkreten Anlass ist es dem Disziplinarvorgesetzten nach Beteiligung der zuständigen Personalvertretung möglich, eine personenbezogene Zuordnung zu erlangen. Die betroffenen Personen sind darüber vorbehaltlich der Beachtung disziplinarrechtlicher Vorschriften nachträglich über den Umfang und den Inhalt der Datenerhebung zu unterrichten.
Sowohl die dienstliche als auch die private Nutzung des Internets inklusive der Protokollierung und der Kontrollen durch den Disziplinarvorgesetzten werden den Bediensteten in einer zu unterzeichnenden Erklärung (Einwilligung) zur Kenntnis gegeben, die zur Personalakte gegeben wird.
E-Mail:
Die Dienstvereinbarung „… über die private Nutzung dienstlicher IT-Systeme einschließlich des dienstlichen Internet-Zugangs und des dienstlichen E-Maildienstes“ erklärt die private

Nutzung des dienstlichen E-Mail-Postfachs für unzulässig. Eine technische oder organisatorische Überwachung dieses Verbotes erfolgt nicht.
Die Dienstvereinbarung „… über die Organisation des IT-Einsatzes…“ regelt die Zugriffberechtigungen wie folgt:
Der Zugriff auf die Inhalte der persönlichen Postfächer einschließlich diesbezüglicher Datensicherungen ist grundsätzlich nur für den Postfachinhaber und von diesem Berechtigte möglich. Ausnahmen bedürfen der Genehmigung durch diejenige Stelle, die die Dienstaufsicht über die Bedienstete oder den Bediensteten innehat, deren bzw. dessen Postfach übernommen werden soll. Die Ausnahmegenehmigung darf erteilt werden, wenn entweder das dienstliche Interesse an der Aufrechterhaltung des Geschäftsbetriebes oder der Gewährleistung der Unversehrtheit von IT-Systemen oder Daten im Falle konkreter IT-Sicherheitsbedrohungen die berechtigten Interessen der Bediensteten oder des Bediensteten an der Datenhoheit erheblich übersteigt. Die bzw. der Bedienstete ist von der Dienstaufsicht führenden Stelle über die Erteilung der Ausnahmegenehmigung unverzüglich zu unterrichten. Die Einrichtung von Weiterleitungen obliegt vorbehaltlich vorstehender Ausnahmegenehmigung ausschließlich der Bediensteten bzw. dem Bediensteten.

Seit Dezember 2016 existiert eine Dienstanweisung für Informationssicherheit im **Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz** und seit Juni 2017 eine Dienstvereinbarung zur privaten Nutzung von dienstlichen IT-Systemen.

Videoüberwachung

Videobeobachtung durch öffentliche Stellen

(TB, Seiten 152 bis 153)
Die LfD erläutert zu diesem Thema die datenschutzrechtlichen Anforderungen bei verschiedenen Stellen wie Schulen und Gerichtsgebäuden.
Die Rechtsauffassung der LfD im Schulbereich wird geteilt. Das Kultusministerium und die Landesschulbehörde beraten die Schulen entsprechend.
Auch zur Videoüberwachung in Gerichtsgebäuden wird die Auffassung der LfD geteilt. Der Tätigkeitsbericht wird zum Anlass genommen, den Geschäftsbereich entsprechend zu sensibilisieren.

Videoüberwachung in öffentlichen Verkehrsmitteln

(TB, Seite 154 bis 159)
Die LfD erläutert die Rechtsauffassung der Datenschutzaufsichtsbehörden zur Zulässigkeit einer Videoüberwachung in öffentlichen Verkehrsmitteln. Dieses Thema wurde bereits in ihrem Bericht für den Zeitraum 2013 bis 2014 ausführlich behandelt, auch bezüglich der im ak-

tuellen Bericht erneut aufgeführten Aspekte zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahmen.
Die Landesregierung teilt die Rechtsauffassung der LfD hierzu nach wie vor nicht und verweist, soweit es sich um Wiederholungen handeln würde, auf ihre Stellungnahme zum vorangegangenen Bericht vom 26.05.2016 (Landtagsdrucksache 17/5855).

Inzwischen hat das Oberverwaltungsgericht Lüneburg (OVG) mit Urteil vom 07.09.2017 – 11 LC 59/16 - entschieden, dass die Videoüberwachung in den Stadtbahnen und Bussen der ÜSTRA (Hannoversche Verkehrsbetriebe AG) mit dem Datenschutzrecht vereinbar ist. Nach Auffassung des OVG ist das Verkehrsunternehmen eine nicht öffentliche Stelle im Sinne des § 2 Abs. 4 BDSG a. F.. Damit war die Rechtmäßigkeit nach § 6 b BDSG a. F. zu prüfen und nicht, wie zuvor vom Verwaltungsgericht Hannover vertreten, nach dem für öffentliche Stellen geltenden § 25 a NDSG a. F.. Die LfD hatte somit gem. § 38 Abs. 5 Satz 1 BDSG a. F. die Möglichkeit, Maßnahmen zur Beseitigung datenschutzrechtlicher Verstöße anzuordnen. Gegenüber öffentlichen Stellen ließ § 23 NDSG a.F. nur eine Beanstandung des festgestellten Verstoßes zu. Materiell-rechtlich unterscheiden sich die Regelungen zur Videoüberwachung nicht wesentlich.

Nach dem Urteil des OVG begründen die von dem Unternehmen festgelegten Zwecke der Videoüberwachung (Verfolgung von Straftaten und der Verhütung von Straftaten, die im Zusammenhang mit der Fahrgastbeförderung stehen) berechtigte Interessen nach § 6 b Abs. 1 S. 1 Nr. 3 BDSG a. F. und sind auch in dem praktizierten Umfang erforderlich. Bezüglich des subjektiven Sicherheitsbedürfnisses der Fahrgäste hat das OVG bestätigt, dass dieses ebenfalls die Videoüberwachung in Bussen und Stadtbahnen rechtfertigt. Da das berechtigte Interesse objektiv begründbar sein muss, kann dieser Zweck für sich genommen die Erforderlichkeit der Videoüberwachung allein nicht begründen. Als weiterer Zweck neben den zuvor genannten ist er jedoch anzuerkennen.
Da Störungen während des Betriebs der Fahrzeuge zu allen Tages- und Nachtzeiten und auch im gesamten Streckengebiet auftreten, scheidet eine Begrenzung der Überwachung auf bestimmte Zeiten am Tag und/oder auf bestimmte Strecken als milderes Mittel aus. Eine durchgängige Videoüberwachung ist hier somit rechtmäßig.
Auch sieht das OVG das sogenannte Black-Box-Verfahren als eingriffsschonender gegenüber dem Monitoring-Verfahren an, bei dem die übermittelten Bilder in jedem Fall von Überwachungspersonen unmittelbar betrachtet und ausgewertet werden. Beim Black-Box-Verfahren wird das Bildmaterial unbesehen für 24 Stunden gespeichert und nur im Bedarfsfall ausgewertet. Nach Auffassung des OVG müssen die Interessen der betroffenen Personen hinter die den Tatbestand begründenden Interessen, die auch mit Blick auf das Videoüberwa-

chungsverbesserungsgesetz (BGBl. I S. 968) teilweise von besonderem Gewicht sind, zurücktreten. Den Interessen der betroffenen Personen, die schon aufgrund der regelmäßig kurzen Aufenthaltsdauer im öffentlichen Nahverkehrsmitteln, nicht so stark tangiert sind, wird u. a. mit der kurzen Speicherdauer von 24 Stunden auf nicht vernetzten Computern und der Auswertung nur im begründeten Einzelfall durch besonders legitimierte Personen in gesonderten Räumen Rechnung getragen. Die Voraussetzungen des § 6 b BDSG a. F. für eine zulässige Videobeobachtung liegen somit vor.
Das Urteil des OVG ist noch nicht rechtskräftig. Die LfD hat Beschwerde gegen die Nichtzulassung der Revision erhoben. Das Verfahren ist bei dem Bundesverwaltungsgericht unter dem Aktenzeichen BVerwG 1 B 150.17 anhängig.