daten schutz

Die
Landesbeauftragte
für den Datenschutz
Niedersachsen

22. Tätigkeitsbericht 2013 – 2014

Niedersachsen

22. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2013 – 2014

Herausgeber: Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5, 30159 Hannover
Postfach 221, 30002 Hannover

Verantwortlich: Barbara Thiel

Layout: design@in-fluenz.de
Lavesstraße 20/21, 30159 Hannover

Druck: Druckhaus Pinkvoss GmbH
Landwehrstraße 85, 30519 Hannover

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

Inhaltsverzeichnis

Zu diesem Bericht 9

1. Polizei und Verfassungsschutz

Globale Überwachung durch Geheimdienste:
Datenschutzbeauftragte in großer Sorge 12

„Mindestspeicherfrist" statt Vorratsdatenspeicherung:
Tarnung misslungen, Grundrechtsproblematik bleibt 16

Detektiert, klassifiziert, verschlüsselt, gelöscht:
Wie datenschutzkonform ist die Geschwindigkeitsabschnittsüberwachung „Section Control"? 20

Premiere:
Verfassungsschutz im Auftrage des Landtags kontrolliert 23

Niedersächsischer Verfassungsschutz:
Task Force beanstandet gut ein Fünftel der Personenspeicherungen 24

Mängel seit 2011, fehlende Informationen:
Keine Fortschritte bei den TKÜ-Projekten 27

2. Datenschutz in Kommunen

Neues Bundesmeldegesetz
Datenschutzbeauftragte bei Novellierung niedersächsischer Vorschriften beteiligt 31

Weitergabe von Meldedaten innerhalb der Gemeinde:
Nur zur Erfüllung von Aufgaben erlaubt 33

Meldedatenabgleich für Rundfunkbeiträge:
Gerichte bestätigen Datenübermittlung 35

Reisegewerbekarte:
Keine Datenübermittlung an die Kammern 37

Das Niedersächsische Hunderegister:
Und noch eine staatliche Datenbank 38

3. Schule

Webbasierte Lernplattformen und Whiteboards:
Eindeutige Rahmenbedingungen für Schulen überfällig 40

Microsoft Office 365:
Einsatz in Schulen unzulässig 42

4. Gesundheit und Soziales

Die elektronische Gesundheitskarte:
Zahlreiche Fragen zum Foto 44

Ausstattung von Pflegeheimen:
Aufsicht und Sozialhilfeträger dürfen Daten austauschen 45

Datenschutz und Kindesunterhalt:
Eltern sind zur Auskunft verpflichtet 47

Krebsregistrierung in Niedersachsen:
Meldepflicht und Datenschutz austariert ... 48
Krankenhausinformationssysteme:
Bundesweit einheitliche Orientierungshilfe weiter verbessert ... 50
Datenschutz in medizinischen Forschungsprojekten:
Intensive Beratungsgespräche mit der TMF ... 53

5. Datenschutzbeauftragte in Behörden und Unternehmen

Behördliche Datenschutzbeauftragte:
Kontaktdaten und eigene Mailadresse Mangelware ... 56
Netzwerkpflege:
Wissenstransfer durch NORD–WEST und SÜD–OST ... 57
Betriebliche Datenschutzbeauftragte:
Viele Fragen zu Fachkunde und Interessenkonflikten ... 58

6. Datenschutz in der Wirtschaft

Datenschutz im Kraftfahrzeug:
Gläserne Fahrer im rollenden Rechner ... 60
Geldtransfer-Verordnung:
EU verlangt Daten bei Bareinzahlung ... 63
Rückabwicklung fehlgeleiteter Überweisungen:
Adressenweitergabe nach Fristsetzung zulässig ... 64
Geldwäsche:
Hausverwaltung muss Bank Daten liefern ... 65
Vervielfältigung von Personalausweisen:
Einscannen und Speichern unzulässig ... 67
Schwerpunktprüfung Zeitarbeitsfirmen:
Keine Verstöße festgestellt ... 69
Datenschutz an der Leine:
Haustierversicherung muss alte Rechnungen zurückschicken ... 70
Dreifachpanne:
Versicherung verschickt Unterlagen Dritter ... 71
Unbefugte Weitergabe von Kundendaten:
Wenn zwei sich streiten, freut sich der Dritte nicht immer ... 72
E-Mail an alle, statt E-Mail für Dich:
Datenschutzgerecht nur mittels bcc-Sendeoption ... 74
Führungszeugnisse ehrenamtlicher Übungsleiter:
Was darf der Verein erfahren und speichern? ... 76
Schuldnerdaten:
Keine Werbung durch Nutzung des Internetportals www.insolvenzbekanntmachungen.de ... 78
Selbstauskünfte von Mietinteressenten:
Für Besichtigungstermin reichen die Kontaktdaten ... 81
„Die guten ins Töpfchen, die schlechten ins Kröpfchen" war einmal:
Nutzung bonitätsgeprüfter Adressen für Werbung nicht mehr zulässig ... 82
Datenschutzverstöße und ihre Konsequenzen:
35 Bußgelder festgesetzt ... 84

7. Beschäftigtendatenschutz

Beschäftigtendatenschutz:
Das rechtliche Niveau muss gehalten werden ... 86
Weitergabe von Arbeitnehmerdaten:
Datenübermittlung an Agrar-Zertifizierungsstellen rechtswidrig ... 88
Biometrisches Zugangssystem:
Fingerabdruckscanner in Fensterfirma unzulässig ... 90
Konto beim Arbeitgeber:
Bank darf nicht Mitarbeiterkonten einsehen ... 91

8. Videoüberwachung

Kameras in Bussen und Bahnen:
Unternehmen streben Totalüberwachung an ... 92
Die Datenschutzbeauftragte empfiehlt:
Finger weg von Dashcams ... 96
Kameras im Schlachthof:
Für Hygieneschleuse erlaubt, für Stempeluhr nicht ... 98
Effektiver Datenschutz im Kaufhaus:
Aus 120 Kameras werden 60 ... 101
Videoüberwachung in Einkaufspassage:
Elf Kameras zu viel ... 103
Webcams in touristischen Gebieten:
Blick in den Strandkorb ... 105
Wildwuchs bei Wildkameras:
Videoüberwachung im Wald nur selten zulässig ... 106
Videoüberwachung an Schulen:
Meistens unzulässig ... 107
Videoüberwachte Gerichtsgebäude:
Hinweisschilder oft nicht wahrnehmbar ... 108

9. Europa und internationaler Datenverkehr

Europäische Datenschutzreform:
Ein Ende ist nicht in Sicht ... 110
Internationaler Datenverkehr und Geheimdiensttätigkeit:
Sind die USA (noch) ein „sicherer Hafen“? ... 113
Die Art.-29-Gruppe – das Datenschutzteam für Europa ... 116
Fluggastdaten:
Reisende unter Verdacht ... 118
Verbindliche konzernweite Regelungen:
Zahl der Anträge auf Binding Corporate Rules nimmt zu ... 119

10. Technisch-organisatorischer Datenschutz und Telemedien

10.1 Internet

Wegweisendes EuGH-Urteil zum „Recht auf Vergessenwerden“:
Löschanspruch bei Suchmaschinen stärkt den Datenschutz ... 120
Mobile Endgeräte:
Trackende Datenschnüffler und allwissende Verräter ... 128

Social Media:
Datenschutzbeauftragte setzen Leitplanken 130
Facebook:
Alltagsbegleiter mit üblen Nebenwirkungen 131
Feuerwehreinsätze auf Facebook:
Vorsicht bei der Veröffentlichung von Anschriften und Fotos 136
Trackingtechnik:
Browsermerkmale und Surfverhalten sind begehrtes Informationsgut 138
Biometrische Gesichtserkennung im Internet:
Nur mit Wahrung des Selbstbestimmungsrechts Betroffener! 142
Datenschutzgerechtes Cloud Computing:
Von der Kunst, Wolken transparent zu gestalten 144
Noch ein Vertrauensverlust:
Der Heartbleed-Bug – Sicherheitslücke im Sicherheitsprotokoll 146
Bundesgerichtshof zu Online-Bewertungen:
Ärzte müssen Netzöffentlichkeit dulden 148
Smart-TV, Streaming, Mediatheken, Rückkanal:
Anonymer Medienkonsum zunehmend gefährdet 150

10.2 Spezifische Handlungsfelder in der Landesverwaltung
Informationssicherheit in Behörden und Kommunen gefährdet:
Strategische Neupositionierung dringend erforderlich 153
TK-Infrastruktur, e-Akte, Anonymisierung, Verschlüsselung:
Beratende Funktion im Niedersächsischen IT-Planungsrat 165
Informationssicherheitsrichtlinie E-Mail:
Innenministerium streicht Versandverbot für besonders schützenswerte Daten 169
Windows 8.1 in der Landesverwaltung:
Kein Konzept gegen neue Bedrohungen 172
Dataport und seine Kunden:
Datenschutzbeauftragte weiter auf Abstimmungs- und Lösungskurs 175
Probleme mit der Mandantenfähigkeit:
Projekt „Cloud-E-Mail“ ohne Niedersachsen 180
E-Mailverkehr in der Justizverwaltung:
Ende-zu-Ende-Verschlüsselung zwingend nötig 182
Elementare Gewährleistungsziele:
Das Standard-Datenschutzmodell nimmt Konturen an 184
Vernichtung von Datenträgern:
Handlungsempfehlung baut Brücke zwischen Datenschutz und DIN 66399 187

11. Datenschutzinstitut Niedersachsen
Fortbildungsbedarf nimmt weiter zu 188

12. Neue Aufgabe!?
Ein Informationszugangs- und Transparenzgesetz für Niedersachsen 190

Zu diesem Bericht

Nur wenige Monate nach dem Erscheinen des XXI. Tätigkeitsberichts im Mai 2015, der sich auf die Berichtsjahre 2011 und 2012 bezieht, lege ich nunmehr den 22. Tätigkeitsbericht für die Jahre 2013 und 2014 vor. Es ist sicher ungewöhnlich, innerhalb eines Jahres zwei Berichte zu erstellen. Die Niedersächsische Verfassung schreibt vielmehr vor, dass die Landesbeauftragte für den Datenschutz „nur" alle zwei Jahre dem Landtag berichten muss. Aber – und das erklärt die aktuellen Besonderheiten – erst mit dem vorliegenden Bericht wird dieser zweijährige Rhythmus wieder aufgenommen.

Am 19. Dezember 2014 hat mich der Niedersächsische Landtag für die Dauer von acht Jahren zur Landesbeauftragten für den Datenschutz gewählt, und am 1. Januar 2015 habe ich mein Amt angetreten. Auch die Berichtsjahre 2013 und 2014 fallen daher noch in den Verantwortungsbereich meines Amtsvorgängers, Joachim Wahlbrink. Ihm danke ich an dieser Stelle für seine Arbeit. Mein besonderer Dank gilt aber den Mitarbeiterinnen und Mitarbeitern in meinem Haus. Ihr engagierter und unermüdlicher Einsatz für die Interessen des Datenschutzes bildet die Grundlage für diesen Tätigkeitsbericht.

Die Themenvielfalt des aktuellen Berichts ist erneut beeindruckend und macht einmal mehr deutlich, dass die Verwendung personenbezogener Daten inzwischen alle Lebensbereiche erfasst. Der Wunsch der Wirtschaft, aber auch des Staates, immer mehr persönliche Daten zu sammeln und nutzen zu können, ist ungebrochen. Daten sind ein Wirtschaftsgut, mit dem sich sehr viel Geld verdienen lässt. Umso wichtiger wird zukünftig die Aufgabe der Datenschutzbehörden, im Vorfeld Aufklärungsarbeit für Bürgerinnen und Bürger zu leisten, auf mögliche Gefahren hinzuweisen und so den unverzichtbaren Selbstdatenschutz stärker in den Vordergrund zu rücken.

Eine immer größere Bedeutung gewinnt die Berücksichtigung datenschutzrechtlicher Anforderungen schon bei der Entwicklung von Produkten. Ich halte es für absolut notwendig, dass dieser Privacy-by-Design-Ansatz bereits in einem sehr frühen Stadium der Produktplanung beachtet wird. Dadurch kann verhindert werden – und das zahlt sich letztlich auch für die Unternehmen aus –, dass Schutzmaßnahmen mit überhöhtem Aufwand in späteren Betriebsphasen nachgebessert werden müssen. Stattdessen sollte bereits in der Designphase, zum Beispiel bei Betriebssystemen, Datenbanken oder auch bei der Entwicklung von Entertainmentplattformen in Autos, die Grundlage für belastbare Datenschutz- und Informationssicherheitskonzepte geschaffen werden.

Autos sind gerade ein gutes Beispiel für die vor einigen Jahren noch undenkbaren Möglichkeiten, die das Internet und die Technik heute bieten. Die Hersteller haben sich dem Ziel verschrieben, Autos immer stärker zu vernetzen und schließlich das autonome Auto auf den Straßen rollen zu lassen. Es wird schon sehr bald zum Standard jedes Fahrzeugs gehören, dass es über eine Internetverbindung verfügt. Damit wird Autofahren zweifellos sicherer und komfortabler. Verkehrszeichen werden erkannt, Staus automatisch umfahren. Aber diese schöne neue Welt hat auch ihre Tücken. Durch die Verbindung zum Internet wird eine Vielzahl von personenbezogenen Daten erhoben und verarbeitet, die sich zu einem umfassenden Persönlichkeitsprofil des Fahrers bzw. des Halters zusammenfügen lassen. Damit sind diese Datensammlungen nicht nur für die Automobilhersteller interessant, sondern ebenso für Kreditfirmen, Scoringunternehmen, Versicherungen oder den Arbeitgeber. Aus Sicht des Datenschutzes ist dabei ein Aspekt nicht verhandelbar: Die Daten gehören dem Halter bzw. dem Fahrer. Er muss mit Blick auf das Grundrecht der informationellen Selbstbestimmung selbst entscheiden können, was mit den Daten geschieht.

Das Grundrecht auf informationelle Selbstbestimmung hat der EuGH durch ein Urteil vom 13. Mai 2014 maßgeblich gestärkt. Suchmaschinenbetreiber wie Google werden damit in die Pflicht genommen. Jeder von uns weiß: Mithilfe von Suchmaschinen lässt sich schnell und ohne Aufwand ein mehr oder weniger detailliertes Profil einer Person erstellen. Die Eingabe von Vorname und Name in das Suchfeld genügt. Mit seiner Entscheidung hat der EuGH dem Schutz der eigenen Daten und der Privatsphäre einen grundsätzlichen Vorrang vor den wirtschaftlichen Interessen der so genannten Intermediäre eingeräumt und diese verpflichtet, Links zu persönlichen, sensiblen Daten aus ihrer Ergebnisliste auf Antrag eines Nutzers zu löschen. Damit ist der Weg frei für das politisch vielfach diskutierte „Recht auf Vergessenwerden“ im Internet.

Insbesondere mit Blick auf immer neue Technologien, die Einzug in unser Leben halten, gilt es, den Schutz des Rechts auf informationelle Selbstbestimmung weiter zu stärken. Hier ist vor allem der europäische Gesetzgeber gefordert, denn Daten machen vor Ländergrenzen nicht halt. Daher begrüße ich es ausdrücklich, dass die ins Stocken geratenen Verhandlungen zur Datenschutz-Grundverordnung im letzten Jahr wieder Fahrt aufgenommen haben und ein Regelwerk geschaffen werden soll, das erstmals europaweit ein einheitliches Datenschutzniveau festlegt. Allerdings ist eine gewisse Skepsis angebracht, denn noch scheint mir nicht sichergestellt zu sein, dass der hohe Standard des deutschen Datenschutzes erhalten bleibt.

Ein Feld mit beängstigend hohem Gefahrenpotential ist die Informationssicherheit. Die globale Überwachung durch Nachrichtendienste unter anderem mittels PRISM, Keyloggern, Backdoors und Trojanern hat gezeigt, wie fragil die Schutzmechanismen gegen Ausspähung tatsächlich sind. Das Land und die Kommunen stehen vor der großen Pflichtaufgabe, die IT-Architektur wirksamer gegen

Angriffe zu wappnen, nicht zuletzt durch den Einsatz sicherer Hard- und Software und durch eine konsequente Ende-zu-Ende-Verschlüsselung.

Datenschutzverstöße beruhen in der Regel auf Unkenntnis, nicht auf Böswilligkeit. Daher erfüllt das in meine Behörde integrierte Datenschutzinstitut Niedersachsen (DsIN) als Schulungs- und Fortbildungseinrichtung für die behördlichen Datenschutzbeauftragten eine wichtige Funktion. Die Vermittlung von rechtlichem Basiswissen auf dem Gebiet des Datenschutzes und der Datensicherheit wird sicherlich auch weiterhin eine wichtige und zentrale Rolle spielen. Zunehmend müssen wir jedoch feststellen, dass die rasante technologische Entwicklung auch den Arbeitsalltag in der öffentlichen Verwaltung nachhaltig beeinflusst. Die datenschutzrechtliche Bewertung vieler Vorgänge steht und fällt nicht selten mit dem Verstehen und dem Durchdringen der Entwicklungen in der IT-Landschaft. Technologisches Fachwissen ist also mehr denn je gefragt und wird deshalb auch weiterhin und verstärkt in den Fortbildungsangeboten am DsIN Berücksichtigung finden.

Sehr geehrte Leserin, sehr geehrter Leser,

ich bin davon überzeugt, dass dieser Tätigkeitsbericht erneut einen wichtigen Beitrag dazu leistet, das Bewusstsein für den Datenschutz nicht nur in Niedersachsen zu schärfen. Nehmen Sie sich Zeit für die Lektüre – es lohnt sich!
Versprochen!

Barbara Thiel
Landesbeauftragte für den Datenschutz

1. Polizei und Verfassungsschutz

Globale Überwachung durch Geheimdienste: Datenschutzbeauftragte in großer Sorge

Ab Juni 2013 hatten unter anderem der Guardian und die Washington Post damit begonnen, den NSA-Skandal zu enthüllen. Dabei wurde bekannt, dass die NSA und andere westliche Geheimdienste in großem Umfang internationale Kommunikation abgreifen und Unternehmen sowie staatliche Stellen ausspionieren. Einzelheiten dieses totalen Überwachungssystems enthüllen streng geheime Dokumente, die der Whistleblower und ehemalige NSA-Analyst Edward Snowden an sich gebracht und an die Medien weitergegeben hatte. Die deutschen Datenschutzbeauftragten verfolgen diese bislang verborgenen Aktivitäten der Nachrichtendienste mit großer Sorge.

In den Jahren des Berichtszeitraumes war dieses Thema immer wieder Gegenstand von ausgiebigen Beratungen bei den regelmäßigen Konferenzen der Datenschutzbeauftragten des Bundes und der Länder (DSK). Ihre Forderungen an Regierungen und Parlamente haben sie in einer ganzen Reihe von Entschließungen zu den unterschiedlichen Aspekten dieser umfassenden weltweiten Kommunikationsüberwachung öffentlich gemacht.
Die erste dazu gefasste Entschließung vom 5. September 2013[1], erinnerte an einen Grundsatz, der zum Fundament einer freiheitlichen Gesellschaft gehört: Es dürfe „keine umfassende und anlasslose Überwachung durch Nachrichtendienste geben", lautete der Titel, verbunden mit der Forderung, dass es „Zeit für Konsequenzen" sei, da drei Monate nach den ersten Enthüllungen offenkundig noch immer nicht alles getan worden war, um das Ausmaß der nachrichtendienstlichen Ermittlungen mithilfe von Programmen wie PRISM, TEMPORA und XKEYSCORE für die Bundesrepublik Deutschland aufzuklären. Erkennbar war bereits, dass globale und tendenziell unbegrenzte Überwachung der Internetkommunikation stattfindet und große Internet- und Telekommunikationsunternehmen in die Geheimdienstaktionen eingebunden sind. Da zahlreiche Anbieter von Kommunikationsdienstleistungen, deren Server in den USA stehen, auch

1 „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen", Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5. September 2013, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9292.de

personenbezogene Daten der Menschen in der Bundesrepublik Deutschland verarbeiten, betreffen die Berichte, dass US-amerikanische Geheimdienste auf dem Territorium der USA personenbezogene Daten umfassend und anlasslos überwachen, auch die Daten hierzulande. Die staatliche Pflicht zum Schutz der Grundrechte erfordert es, sich nicht mit der gegenwärtigen Situation abzufinden.

Es geht um das Grundvertrauen in den Rechtsstaat

Die DSK forderte daher alle Verantwortlichen auf, die notwendigen Konsequenzen zügig zu treffen, da es um nicht weniger als das Grundvertrauen der Bürgerinnen und Bürger in den Rechtsstaat geht. Dazu gehört, nationales, europäisches und internationales Recht – einschließlich völkerrechtlicher Abkommen – so weiterzuentwickeln und umzusetzen, dass es einen umfassenden Schutz der Privatsphäre, der informationellen Selbstbestimmung, des Fernmeldegeheimnisses und des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme garantiert. Zudem muss die Kontrolle der Nachrichtendienste verbessert werden. Aber auch die technisch-organisatorischen Maßnahmen müssen geprüft und ausgebaut werden, wie zum Beispiel

- gesteuertes Routing von Telekommunikationsverbindungen,
- der Ausbau anonymer Nutzungsmöglichkeiten von Telekommunikationsangeboten und
- die Schaffung von Voraussetzungen für eine objektive Prüfung von Hard- und Software durch unabhängige Zertifizierungsstellen.

Kryptographische Verfahren sind Pflicht

In einer zweiten Entschließung vom 1. und 2. Oktober 2013[2] ergänzte die DSK den ersten Appell um die Forderung, eine sichere elektronische Kommunikation zu gewährleisten und eine Ende-zu-Ende-Verschlüsselung einzusetzen und weiterzuentwickeln. Für die elektronische Datenübermittlung zwischen den Bürgerinnen und Bürgern beziehungsweise der Wirtschaft und der öffentlichen Verwaltung im Zusammenhang mit E-Government-Verfahren müssen zur Sicherung der Vertraulichkeit, Integrität, Authentizität, Zweckbindung und Transparenz kryptographische Verfahren in Form von Ende-zu-Ende-Verschlüsselung und Verbindungsverschlüsselung eingesetzt werden. Beide Ansätze ergänzen sich, deshalb hält die DSK den Einsatz von Standards zur Ende-zu-Ende-Verschlüsselung wie OSCI-Transport für geboten und fordert den IT-Planungsrat auf, diese kontinuierlich weiterzuentwickeln und verbindlich festzulegen. Daneben sind Bund, Länder und Kommunen aufgefordert, die vorhandenen Standards bereits jetzt einzusetzen.

Gewährleistung der Menschenrechte

Die dritte Entschließung der DSK vom 27. und 28. März 2014[3] befasste sich erneut mit der „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“ und konkretisierte technisch-organisatorische Maßnahmen in einem Zwölf-Punkte- Anforderungskatalog. Dazu gehören

- die vorgenannte Verschlüsselung,
- eine Infrastruktur dafür,
- Internetangebote mit verbesserter IT-Sicherheit und Vertrauenswürdigkeit,
- weiterentwickelte Schutzmaßnahmen für Verkehrsdaten,
- anonyme Kommunikation,
- kontrolliertes Routing in Netzen,
- sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung,

2 „Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln“, Entschließung der 86. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. und 2. Oktober in Bremen, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9328.de

3 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation“, Entschließung mit Anlage der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. und 28. März 2014 in Hamburg, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9475.de und Anlage zur Entschließung mit 12-Punkte-Katalog: https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9510.de

- Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit,
- Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung,
- Sensibilisierungsmaßnahmen für Nutzerinnen und Nutzer der Technik sowie
- eine ausreichende Finanzierung von Maßnahmen der Informationssicherheit.

Die DSK richtete ihre Forderungen hierzu an drei Adressaten: Die Anbieter elektronischer Kommunikationsdienste sollen entsprechende Technologien und Dienste zur Verfügung stellen, die Verwaltungen in Bund und Ländern, insbesondere die zuständigen Regulierungsbehörden, sollen auf die Durchsetzung der vorgenannten Maßnahmen dringen, und der Gesetzgeber ist aufgerufen, die zu ihrer Durchsetzung gegebenenfalls nötigen Änderungen und Präzisierungen an dem bestehenden Rechtsrahmen vorzunehmen.

DSK fordert mehr Prüfbefugnisse

In einer vierten Entschließung vom 8. und 9. Oktober 2014[4] zu diesem Themenkomplex konzentrierte sich die DSK auf die Rolle deutscher Nachrichtendienste und forderte, die effektive Kontrolle von Nachrichtendiensten herzustellen. Die Enthüllungen über die Spähaktivitäten ausländischer Nachrichtendienste hatten vor Augen geführt, welche ungeheuer großen Mengen von Kommunikationsdaten in der digitalisierten Welt anfallen, welche Begehrlichkeiten diese Daten offensichtlich bei Nachrichtendiensten selbst demokratischer Länder wecken und mit welchen weitreichenden Methoden die Nachrichtendienste Informationen erfassen, sammeln und analysieren. Auch die deutschen Nachrichtendienste haben weitreichende Befugnisse zur Erhebung, Sammlung und Auswertung personenbezogener Daten sowie zum Austausch dieser untereinander und mit Polizeibehörden. Die Befugnisse der Nachrichtendienste schließen auch die Überwachung der Telekommunikation ein. Damit einher geht im Bereich der strategischen Auslandsüberwachung des BND ein Kontrolldefizit.
Die Berichte der NSU-Untersuchungsausschüsse des Deutschen Bundestages und einiger Landesparlamente haben darüber hinaus erhebliche Kontrolldefizite auch bei den Verfassungsschutzämtern offengelegt. Nach Einschätzung der DSK ist daher eine Reform der rechtsstaatlichen Kontrolle der deutschen Nachrichtendienste dringend geboten. Auch das Bundesverfassungsgericht hat mit der Entscheidung vom 24. April 2013 zum Zusammenwirken zwischen den Datenschutzbeauftragten und den parlamentarischen Kontrollinstanzen festgestellt: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“ Die DSK forderte daher den Gesetzgeber auf, die Datenschutzbehörden mit entsprechenden Prüfbefugnissen auszustatten, damit das bei ihnen vorhandene Fachwissen auch in diesem Bereich genutzt werden kann.

4 „Effektive Kontrolle von Nachrichtendiensten herstellen!“, Entschließung der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014, https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.9636.de

„Mindestspeicherfrist“ statt Vorratsdatenspeicherung: Tarnung misslungen, Grundrechtsproblematik bleibt

Das zähe Ringen um die Frage, wie lange der Staat Informationen über die Verkehrsdaten aller Telekommunikationsanschlüsse (TK-Anschlüsse) anlasslos und ohne Anfangsverdacht einer schweren Straftat auf Vorrat speichern darf oder durch Provider speichern lassen darf, ist trotz der Urteile des Bundesverfassungsgerichts und des Europäischen Gerichtshofs noch immer nicht beendet. Auch ein verändertes Vokabular („Mindestspeicherfristen bei den TK-Verkehrsdaten“ statt Vorratsdatenspeicherung) kann nicht über die Grundrechtsproblematik hinwegtäuschen.

Mit einer Vorratsdatenspeicherung wird massiv in die Freiheitsrechte aller Menschen, unabhängig von einem konkreten Verdacht, eingegriffen. Deshalb müssen derartige Maßnahmen, die nur als absolute Ausnahme überhaupt zulässig sein können, einer strengen Prüfung hinsichtlich Erforderlichkeit und Verhältnismäßigkeit unterzogen und durch technische, organisatorische und verfahrensrechtliche Vorkehrungen abgesichert werden. Diese grundlegende Haltung nehmen nicht nur die Datenschutzbeauftragten von Bund und Ländern seit Jahren ein, sie spiegelt sich auch in der laufenden Rechtsprechung des Bundesverfassungsgerichtes (BVerfG) wider. Im XX. Tätigkeitsbericht für die Jahre 2009–2010[1] berichtete mein Vorgänger umfänglich über den Werdegang des gesetzlichen Vorstoßes seit 2006 und über die inhaltlichen Fragen des Grundrechtsschutzes, die sich bei der gesetzlichen Normierung einer TK-Verkehrsdatenspeicherung stellen. Dabei ist weiterhin zu konstatieren, dass nur wenige andere Themen in der Geschichte des Datenschutzes so langandauernd und intensiv zu gesellschaftlichen und rechtspolitischen Auseinandersetzungen geführt haben, wie die Kontroverse zu diesem Thema. Neben der Komplexität der rechtlichen Fragen und der technisch-organisatorischen Risiken ist die extreme und unversöhnliche Gegensätzlichkeit der Rechtsauffassungen ein Grund für diese intensive datenschutzpolitische Diskussion.

Gutachten stellen Wirksamkeit in Frage

Bemerkenswert ist, dass die Bundesregierungen bis zum Ende des Berichtszeitraumes 2014 nicht hinreichend begründet hatten, warum die Speicherung von Standortdaten und Kommunikationsdaten tatsächlich erforderlich ist, zumal die Gutachten des Max-Planck-Instituts vom Juli 2011 im Auftrag des Bundesamtes für Justiz[2] und der Wissenschaftlichen Dienste des Deutschen Bundestages vom Februar 2011[3] die Wirksamkeit der Maßnahme in

1 Siehe XX. Tätigkeitsbericht 2009–2010, Kapitel 3 „Vorratsdaten: Totalspeicherung ohne Anfangsverdacht“, Seite 78

2 Das Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht im Auftrag des Bundesamtes für Justiz zu möglichen Schutzlücken durch den Wegfall der Vorratsdatenspeicherung, 2. erweiterte Fassung, Freiburg i. Br., Juli 2011, wurde dem Rechtsausschuss des Bundestags am 27.1.2012 vorgelegt. https://www.mpicc.de/de/forschung/forschungsarbeit/kriminologie/vorratsdatenspeicherung.html, Volltext http://www.mpg.de/5000721/vorratsdatenspeicherung.pdf

3 Wissenschaftliche Dienste des Deutschen Bundestages, „Ausarbeitung zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta“, Dr. Roland Derksen, WD 11 – 3000 – 18/11

Frage gestellt hatten. Bei allem Streit über die Qualität dieser Datensammlung ist es weiterhin problematisch, dass die Befürworter eine ernsthafte Abwägung zwischen den staatlichen Befugnissen im Bereich der inneren Sicherheit (Strafprozessrecht und Gefahrenabwehrrecht) einerseits und den Grundsätzen freier Mediennutzung und den Persönlichkeitsrechten andererseits, wie vom Bundesverfassungsgericht gefordert, schuldig bleiben. Letztlich muss sich jede gesetzliche Lösung am Verfassungsrecht und am europäischen Menschenrechtsrahmen messen lassen.

Nach dem Urteil des BVerfG vom 2. März 2010[4] hätte diese rechtspolitische Diskussion eigentlich beendet sein können. Hier entschied das Gericht einmal mehr im Sinne der Stärkung des Rechts auf informationelle Selbstbestimmung als Bestandteil des Persönlichkeitsrechts und bescheinigte dem Gesetzgeber unzulängliche Grundrechtsabwägungen. Die Entscheidung über das Gesetz zur Umsetzung der entsprechenden EU-Richtlinie lautete im Tenor, dass die Regelungen der §§ 113 a Abs. 1, 113 b Satz 1 Telekommunikationsgesetz (TKG) sowie § 100 g Strafprozessordnung (StPO), soweit danach Verkehrsdaten nach § 113 a TKG erhoben werden dürfen, einen Verstoß gegen das Telekommunikationsgeheimnis gemäß Art. 10 Abs. 1 Grundgesetz darstellten. Die Karlsruher Richter erklärten die Vorschriften nicht nur für verfassungswidrig, sondern für nichtig und ordneten die unverzügliche Löschung der bereits gespeicherten Vorratsdaten an. Damit verhängte das Gericht die schärfste ihm zur Verfügung stehende Sanktion gegen einen verfassungswidrigen Rechtsakt des Gesetzgebers.

Statt in der Konsequenz des Urteils das Vorhaben, die anlasslose Vorratsdatenspeicherung über die Persönlichkeitsrechte zu stellen, aufzugeben, verfolgten vor allem Innenpolitiker weiter das Ziel, mit einer Neuauflage einer gesetzlichen Regelung eine TK-Verkehrsdatenspeicherung anlassfrei und auf Vorrat für die Strafverfolgung wieder einzuführen. Begründung: Das BVerfG habe dieses Instrument nicht vollkommen ausgeschlossen.

Koalitionsvertrag ignoriert DSK-Entschließung

Während des Bundestagswahlkampfs 2013 war in Deutschland auch die Vorratsdatenspeicherung ein Thema, deren Zukunft nach dem Wahlausgang von den Koalitionsparteien und deren Verhandlungsergebnissen abhing. In einer Entschließung[5] forderte daher die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) im Oktober 2013 erneut, den Grundrechtsschutz nicht zu schwächen, sondern zu stärken: „Die Konferenz erwartet von der Bundesregierung außerdem, dass sie sich für die Aufhebung der EU-Richtlinie zur anlasslosen Vorratsdatenspeicherung von Telekommunikationsdaten einsetzt."

Der Koalitionsvertrag zwischen CDU, CSU und SPD für die 18. Legislaturperiode vom 14. Dezember 2013[6] traf gleichwohl die politische Festlegung, die Vorratsdatenspeicherung nach dem EU-Recht in nationale Gesetzgebung umzusetzen.

4 Urteil des BVerfG, 1 BvR 256/08 vom 2. März 2010, Absatz-Nr. (1–345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08)

5 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. bis 2. Oktober 2013 in Bremen: „Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages"

6 Koalitionsvertrag zwischen CDU, CSU und SPD für die 18. Legislaturperiode vom 14. Dezember 2013, downloadbar bei der CDU https://www.cdu.de/artikel/der-koalitionsvertrag-von-cdu-csu-und-spd oder bei der SPD https://www.spd.de/scalableImageBlob/112790/data/20131127_koalitionsvertrag-data.pdf oder bei der CSU http://www.csu.de/aktuell/meldungen/2013/dezember-2013/unterzeichnung-des-koalitionsvertrags/, Seiten 102 f.

Sitz des Europäischen Gerichtshofs in Luxembourg (Quelle: Wikipedia)

Europäischer Gerichtshof erklärt Richtlinie für ungültig

Mit seinem Urteil[7] zur Richtlinie über die Vorratsdatenspeicherung[8] stellte der Europäische Gerichtshof (EuGH) klar, dass den datenschutzsichernden Grundrechten eine hohe Bedeutung zukommt. Im Tenor erklärten die Richter diese Richtlinie für europarechtswidrig und sogar rückwirkend für unwirksam, weil damit unzulässig in Grundrechte, insbesondere in das Telekommunikationsgeheimnis, eingegriffen werde und die Richtlinie zudem einen „Eingriff von großem Ausmaß und besonderer Schwere in die Grundrechte auf Achtung des Privatlebens und auf den Schutz personenbezogener Daten beinhalte, der sich nicht auf das absolut Notwendige" beschränke. Der durch die Richtlinie bedingte schwerwiegende und unverhältnismäßige Eingriff in die Grundrechte stelle einen Verstoß gegen Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union dar. Kritisch sah das Gericht insbesondere die unzureichenden Vorgaben und fehlenden Konkretisierungen in der Richtlinie, die vor allem hinsichtlich der weitreichenden Auswirkungen und der Aussagekraft, die eine umfassende Überwachung des Telekommunikationsverhaltens sämtlicher EU-Bürgerinnen und -Bürger mit sich bringe, hätten festgelegt werden müssen.
Deutlich kritisierte der EuGH:

- Die Richtlinie solle dem Ziel der Bekämpfung schwerer Kriminalität dienen, sehe aber keinerlei Beschränkungen der erfassten Daten oder Personen vor, die zur Erreichung dieses Zieles tatsächlich benötigt würden. Vielmehr rechtfertige sie eine pauschale Speicherung sämtlicher Kommunikationsvorgänge und damit sogar solcher, die dem besonderen rechtlichen Schutz von Berufsgeheimnisträgern unterlägen.
- Die Richtlinie stelle auch weder objektive Kriterien für eine notwendige Beschränkung der Zugangsberechtigten zu den Vorratsdaten auf, noch verlange sie eine Vorabkontrolle des Zugangs zu den Daten durch eine unabhängige Stelle oder ein Gericht.
- Die vorgesehene Speicherfrist von sechs bis 24 Monaten sei ohne Vorgabe konkreter Kriterien festgesetzt worden, die eine Beschränkung der Speicherdauer auf das absolut Notwendige vorsähen.
- Die Richtlinie schreibe zudem keine Speicherung der Daten innerhalb des Unionsgebietes vor, so dass die zwingend notwendige und in der Grundrechtecharta explizit geforderte unabhängige Datenschutzaufsicht nicht vollumfänglich gewährleistet sei.

7 Urteil des Europäischen Gerichtshofes (EUGH) vom 8. April 2014, Az. C-293/12 und C-594/12, http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62012CJ0293&qid=1401730612197&from=DE

8 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die eine anlasslose und massenhafte Speicherung von TK-Verkehrsdaten stets abgelehnt hatte[9], begrüßte am 25. April 2014[10] mit der Entschließung „Ende der Vorratsdatenspeicherung in Europa!" die Entscheidung des EuGH als wichtigen Schritt zur Bekräftigung der informationellen Selbstbestimmung und des Telekommunikationsgeheimnisses. Da das Urteil die Richtlinie für unwirksam erklärt hat, liegt keine Rechtsgrundlage für die Vorratsdatenspeicherung mehr vor. Die darauf fußenden Regelungen in den Mitgliedsstaaten entbehren damit ebenfalls der Grundlage.

Diskussion um Neuauflage nicht beendet

Im politischen Raum setzte sich nach dem Urteil gleichwohl die Diskussion fort, ob und wie eine Vorratsdatenspeicherung künftig geregelt werden sollte und könnte. Besonders von Seiten der Innenpolitiker sowie Vertretern von Ermittlungs- und Strafverfolgungsbehörden wurde weiterhin argumentiert, dass eine Vorratsdatenspeicherung mit einer nationalen Rechtsgrundlage für die Kriminalitätsbekämpfung – besonders für Delikte im Internet und mit Hilfe des Tatmittels Internet sowie für schwere Straftaten – unabdingbar sei. Zum Ende des Berichtszeitraums war es allerdings nicht gelungen, zwischen dem Bundesjustizministerium und dem Bundesinnenministerium eine einheitliche Meinungsbildung herbeizuführen.

Besorgniserregend: Vorsorgliche Verhaltensaufzeichnung auf alle Bereiche ausdehnbar

Als Grundproblem sehe ich nach allen Erfahrungen zu der Abwägungsfrage zwischen Sicherheit und Grundrechtsschutz den Effekt eines Dammbruchs. Billigt die Gesellschaft das Konstrukt der vorsorglichen Vorratsdatenspeicherung und führt es durch Rechtsnormen ein, entzieht dies gleichzeitig dem Grundrecht auf informationelle Selbstbestimmung die Grundlage. Denn wenn die flächendeckende Aufzeichnung der Kommunikation oder anderer Aktivitäten aller Personen für legitim erklärt wird, weil man abstrakt oder konkret davon ausgeht, dass Sicherheitsbehörden daran in der Zukunft Interesse oder daraus einen Nutzen entwickeln könnten, dann wäre dieses Konstrukt einer vorsorglichen Verhaltensaufzeichnung sukzessive auf alle Lebensbereiche ausdehnbar. Schließlich ist davon auszugehen, dass es keine Informationen gibt, die irrelevant sind und nicht für Überwachungs- oder Nachweiszwecke taugten. Mit diesem Ansatz aber wären im Endausbau die totale Überwachung, der vollständige Verlust der informationellen Selbstbestimmung und damit eine totale Unfreiheit erreicht. Dieses wäre mit den elementaren Grundsätzen unserer Verfassung schlichtweg nicht vereinbar.

9 Vgl. Entschließungen der Konferenzen der Datenschutzbeauftragten des Bundes und der Länder zwischen 2005 und 2010: 79. Konferenz vom 17./18. März 2010 „Keine Vorratsdatenspeicherung!"; http://www.baden-wuerttemberg.datenschutz.de/konferenzentschliesungen-2010-keine-vorratsdatenspeicherung/ 73. Konferenz am 8./9. März 2007 in Erfurt, „Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen", https://www.tlfdi.de/tlfdi/berichte/entschliessungen_datenschutzkonferenz/archiv/73/vorratsdatenspeicherung/ 70. Konferenz am 27./28. Oktober 2005 in der Hansestadt Lübeck „Keine Vorratsdatenspeicherung in der Telekommunikation", http://www.datenschutz.sachsen-anhalt.de/konferenzen/nationale-datenschutzkonferenz/entschliessungen/entschliessungen-der-70-konferenz-am-2728oktober-2005-in-der-hansestadt-luebeck/keine-vorratsdatenspeicherung-in-der-telekommunikation/

10 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. April 2014 „Ende der Vorratsdatenspeicherung in Europa!", https://ssl.bremen.de/datenschutz/sixcms/media.php/13/Entschlie%DFung_Vorratsdatenspeicherung.pdf

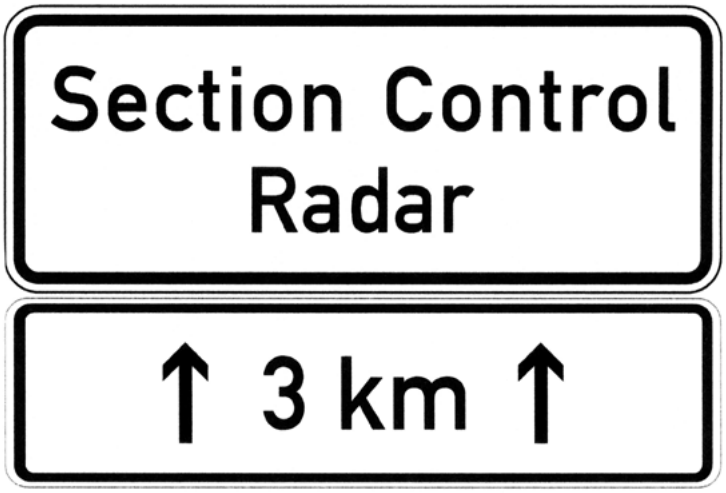
Detektiert, klassifiziert, verschlüsselt, gelöscht: Wie datenschutzkonform ist die Geschwindigkeitsabschnittsüberwachung „Section Control“?

Bereits im Juli 2014 hat mich das Niedersächsische Ministerium für Inneres und Sport an den ersten Planungen für die Erprobung einer Streckengeschwindigkeitsüberwachungsanlage (Section Control) beteiligt, die im Laufe des Jahres 2015 an der Bundesstraße 6 zwischen Gleidingen und Rethen errichtet werden soll. Für eine fundierte Prüfung der technischen Abläufe fehlten mir allerdings bis zum Ende des Berichtszeitraums die erbetenen Unterlagen wie Datenschutzkonzept und Vorabkontrolle.

Das Innenministerium plant die Erprobung eines stationären Systems zur Geschwindigkeitskontrolle auf einem definierten Streckenabschnitt von drei Kilometer Länge. Vergleichbare Anlagen gibt es beispielsweise in Österreich, der Schweiz und in den Niederlanden. Dabei werden von Fahrzeugen, deren Durchschnittsgeschwindigkeit innerhalb des festgelegten Streckenabschnitts höher ist als die zulässige Höchstgeschwindigkeit, so genannte Vorfallsdatensätze mittels des bekannten „Blitzens“ und der damit verbundenen Lichtbildaufnahme des Fahrzeugs einschließlich des Fahrzeugführers generiert, um anschließend die begangene Ordnungswidrigkeit zu ahnden.
Die Feststellung einer Geschwindigkeitsdurchschnittsübertretung erfolgt nach Angaben der Hersteller solcher Anlagen in einer Reihe von Teilschritten: So werden die Fahrzeuge am Ein- und Ausfahrtsquerschnitt der Anlage detektiert, klassifiziert und durch Kameras fotografisch von hinten erfasst. Innerhalb der besonders gesicherten Rechnerkomponenten der Anlage sollen die Heckaufnahmen bereits am Einfahrtsquerschnitt hochverschlüsselt werden, womit eine manuelle Rückführbarkeit auf das amtliche Kennzeichen ausgeschlossen sein soll. Nach dem Durchfahren des Ausfahrtsquerschnitts erhält ein Auswerterechner die entsprechenden Hashwerte des durchfahrenden Fahrzeugs und ermittelt anhand der eingestellten Wegstreckenlänge die Durchfahrtzeit und damit die gefahrene Durchschnittsgeschwindigkeit. Im Fall der Übertretung wird anschließend der Vorfallsdatensatz durch das Auslösen des „Blitzens“ generiert. In allen anderen Fällen soll eine sofortige und unwiderrufliche Löschung der Datensätze erfolgen.

Rechtlich mit Kennzeichenlesegeräten vergleichbar

Das Bundesverfassungsgericht hat in seinem Urteil vom 11. März 2008 (1 BvR 2074/05 und 1 BvR 1254/07) zum Einsatz von Kennzeichenlesesystemen in Hessen und Schleswig-Holstein einen Eingriff in das Recht auf informationelle Selbstbestimmung nicht als gegeben angesehen, wenn das amtliche Kennzeichen unverzüglich mit dem Fahndungsbestand der Polizei abgeglichen und ohne weitere Auswertung sofort wieder gelöscht wird (Leitsatz 1 und Randnummer 68 des Urteils). Auch müsse bei Nichttrefferfällen rechtlich und technisch gesichert sein, dass die Daten anonym bleiben und sofort



spurlos und ohne die Möglichkeit, einen Personenbezug herzustellen, gelöscht werden (Randnummer 68). Natürlich fordert das Bundesverfassungsgericht, ungeachtet der vorstehenden Ausführungen, für die Erfassung der amtlichen Kennzeichen eine gesetzliche Ermächtigungsgrundlage, die den rechtsstaatlichen Anforderungen an die Bestimmtheit und Klarheit genügt (Randnummer 93).
In Anlehnung an dieses Urteil halte ich den Einsatz einer Section Control-Anlage für grundsätzlich zulässig. Zwar gibt es hinsichtlich der Speicherdauer der erhobenen Daten Unterschiede. Wenn jedoch durch technisch-organisatorische Maßnahmen sichergestellt ist, dass die Daten von Nichttreffer-Fällen (die Durchschnittsgeschwindigkeit ergibt keine Überschreitung der zulässigen Höchstgeschwindigkeit) sofort gelöscht werden und bis zur Löschung niemand auf die Daten zugreifen kann, sind die Kernforderungen des Bundesverfassungsgerichts aus meiner Sicht erfüllt. Der Einsatz dieser Anlage ist also, wenn auch mit einer anderen Zielrichtung, rechtlich mit dem Einsatz von Kennzeichenlesegeräten vergleichbar.

Kein Raum für Generalklausel

Nicht einschlägig hingegen ist der vom Innenministerium als Rechtsgrundlage herangezogene § 11 Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG). Diese Generalklausel erlaubt der Polizei, die notwendigen Maßnahmen zur Abwehr einer Gefahr zu treffen. Dies allerdings nur dann, wenn die Befugnisse der Polizei nicht in den „Vorschriften des Dritten Teils“ (des Nds. SOG) besonders geregelt sind. In diesem Dritten Teil sind unter anderem die Befugnisse der Polizei zur Datenverarbeitung umfassend und abschließend geregelt, sodass für die Anwendung der Generalklausel kein Raum mehr bleibt. Zudem sind Maßnahmen der Polizei gegenüber einzelnen Betroffenen immer nur dann möglich, wenn eine konkrete Gefahr vorliegt. Beim Einsatz einer Section-Control-Anlage liegt aber lediglich eine abstrakte Gefahrenlage in Gestalt eines Unfallschwerpunktes vor.

Ich habe mich daher gegenüber dem Innenministerium auf der Grundlage der vorstehend geschilderten Rechtsprechung des Bundesverfassungsgerichts damit einverstanden erklärt, dass in Niedersachsen zu Erprobungszwecken eine Section-Control-Anlage im öffentlichen Verkehrsraum eingesetzt wird, wenn:

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

Diese Grundsätze sind zwingend zu beachten.

Wie sicher sind die Daten vor Hackern und Dieben?

Ferner habe ich das Innenministerium gebeten, zeitgerecht eine detaillierte Vorabkontrolle vorzulegen, aus der insbesondere die technischen Schutzmaßnahmen der Anlage hervorgehen, damit ich mich davon überzeugen kann, dass nach dem Stand der Technik für Hacker oder Diebe keine Möglichkeit besteht, die Datensätze anderweitig zu erlangen oder zu verarbeiten.
Im Rahmen des Projektfortgangs hat mich das niedersächsische Innenministerium und die von ihm mit der Durchführung eines Ausschreibungsverfahrens beauftragte Zentrale Polizeidirektion im Dezember 2014 erneut konsultiert. Dabei wurden Fragen zu maßgeblichen technisch-organisatorischen Schutzmaßnahmen des Datenverarbeitungsverfahrens und der Messanlage erörtert. Einige Antworten darauf sollten im Folgejahr anhand von Lösungen des Gewinners der Ausschreibung gegeben werden. Die Erarbeitung der von mir bereits geforderten Vorabkontrolle und des ebenfalls erbetenen Datenschutzkonzepts durch die verantwortliche Stelle der Polizei wurden für die Folgemonate in Aussicht gestellt.
Über die abschließenden Ergebnisse meiner Prüfung und Beteiligung werde ich zu gegebener Zeit berichten.

Premiere: Verfassungsschutz im Auftrage des Landtags kontrolliert

Lange Zeit schlummerte § 27 Absatz 1 Satz 1 des Niedersächsischen Verfassungsschutzgesetzes (NVerfSchG) im Verborgenen. Nach dieser Vorschrift kann der Ausschuss des Niedersächsischen Landtags für Angelegenheiten des Verfassungsschutzes die oder den Landesbeauftragten für den Datenschutz beauftragen, die Rechtmäßigkeit einzelner Maßnahmen der Verfassungsschutzbehörde zu überprüfen.

Im September 2013 trat § 27 Absatz 1 Satz 1 NVerfSchG dann hervor: Der Landtagsausschuss beauftragte mich, die Speicherung diverser personenbezogener Datensätze in der Verfassungsschutzbehörde auf ihre Rechtmäßigkeit hin ebenso zu überprüfen wie das Vorgehen der Verfassungsschutzbehörde im Umgang mit diesen Daten. Hintergrund dieses Auftrags war die Tatsache, dass die Verfassungsschutzbehörde in Eigeninitiative Speicherungen zu Personen bestimmter Berufsgruppen überprüft hatte und zu dem Ergebnis gekommen war, bestimmte Speicherungen seien rechtswidrig. Dieser Sachverhalt führte letztlich auch zur Einsetzung der so genannten Task Force (siehe Seite 24).

Daten teilweise bereits gelöscht

Zeitweise gestaltete sich die Überprüfung sehr schwierig, da die Behörde die Datensätze zu einem Teil der Personen bereits gelöscht hatte. Hier war es nur noch möglich, Datensätze aufzufinden, die auch bei anderen Personen aufgrund eines inneren Sachzusammenhanges zugespeichert worden waren. Aus diesen Daten allein ergab sich kein Sachverhalt, der darauf schließen ließ, ob diese Speicherungen zu den eigentlich betroffenen Personen rechtmäßig waren oder nicht. Hierzu hätte ich die Gesamtheit aller Daten beurteilen müssen, was allerdings aufgrund der erfolgten Löschungen nicht (mehr) möglich war. Ich konnte deshalb den Ausschuss in diesen Fällen nicht umfassend unterrichten.

Einige Speicherungen unzulässig

In den übrigen Fällen waren noch keine Löschungen erfolgt, die Akten waren lediglich gesperrt worden. In diesen Fällen ergab meine Überprüfung, dass die Speicherungen zu den betroffenen Personen nicht hätten erfolgen dürfen, da die Voraussetzungen für ein Tätigwerden des Verfassungsschutzes (§§ 3 und 5 NVerfSchG) nicht vorgelegen hatten. Hierüber und über die Tatsache, dass das Vorgehen der Verfassungsschutzbehörde im Umgang mit diesen Daten datenschutzrechtlich nicht zu beanstanden war, unterrichtete ich den Ausschuss in vertraulicher Sitzung.

Niedersächsischer Verfassungsschutz: Task Force beanstandet gut ein Fünftel der Personenspeicherungen

Der niedersächsische Innenminister richtete Anfang Oktober 2013 eine Task Force zur Überprüfung des personenbezogenen Datenbestands des niedersächsischen Verfassungsschutzes ein. Sie wurde als unabhängiges Gremium eingesetzt und bestand aus sechs stimmberechtigten Mitgliedern und einer Geschäftsstelle. Darüber hinaus stand mein Vertreter der Task Force in beratender Funktion zur Seite.

Aufgabe der Task Force war es, die in der Amtsdatei des Landesverfassungsschutzes vorhandenen personenbezogenen Speicherungen auf ihre Rechtmäßigkeit hin zu überprüfen und zwar sowohl mit Blick auf die Zulässigkeit der Erstspeicherung als auch in Bezug auf die jetzt noch bestehende Speicherung. Ziel war es, eine neutrale Bewertung der vorhandenen personenbezogenen Speicherungen vorzunehmen und somit zu einer Konsolidierung des Datenbestandes des Verfassungsschutzes zu kommen. Die Geschäftsstelle der Task Force begann am 8. Oktober 2013 zunächst mit vorbereitenden Arbeiten. Die Überprüfung der einzelnen Speicherungen konnte sodann, nach Erteilung der notwendigen Sicherheitsbescheide, am 21. Oktober 2013 beginnen.
Die Überprüfung der Speicherungen erfolgte in einem ersten Schritt durch die Geschäftsstelle der Task Force. Grundlage der Überprüfung waren zunächst die in der Amtsdatei des Verfassungsschutzes gespeicherten Erkenntnisse. Kam diese erste Überprüfung durch die Geschäftsstelle zu dem Ergebnis, dass die Speicherung rechtmäßig ist, erfolgte keine Vorlage an die übrigen Mitglieder der Task Force. Zweifelhafte Fälle sowie solche, die nach Auffassung der Geschäftsstelle rechtlich nicht zulässig oder nicht mehr erforderlich waren, wurden der Gesamt-Task-Force zur Bewertung vorgelegt. Im Zuge der anschließenden Beratung erfolgten bei Bedarf weitere oder ergänzende Einsichtnahmen in die vorhandenen Akten oder es wurde eine Stellungnahme des Fachbereichs eingeholt. Soweit die Gesamt-Task-Force nicht zu einer eindeutigen Bewertung gelangte, wurde mein Vertreter in beratender Funktion beteiligt. Dies war zweimal der Fall. Diesem Ablauf folgend ergingen sämtliche Entscheidungen der Task Force im Ergebnis einvernehmlich.

Drei Löschungskategorien

Der Verbleib eines Datensatzes wurde von der Task Force empfohlen, wenn die Prüfung zu dem Ergebnis gelangte, dass die Erstspeicherung rechtmäßig erfolgt und die Speicherung der betroffenen Person auch gegenwärtig weiterhin erforderlich war. Eine Empfehlung zur Löschung des Datensatzes basierte auf der Bewertung der Task Force, dass die Erstspeicherung rechtswidrig oder die Speicherung zum Zeitpunkt der Über-

prüfung nicht mehr erforderlich war. In diesen Fällen bestand daher nach Auffassung der Task Force gemäß § 10 Abs. 2 Satz 1 Niedersächsisches Verfassungsschutzgesetz (NVerfSchG) eine Verpflichtung zur Löschung der Daten.
Die Empfehlungen zur Löschung von Datensätzen gliederte sich in drei von der Task Force entwickelte Kategorien (A, B, C):

Kategorie A: Rechtswidrigkeit der Speicherung
Eine Löschempfehlung verbunden mit einer Einstufung als Kategorie A beruhte auf der Bewertung der Task Force, dass die Erstspeicherung des entsprechenden Datensatzes rechtswidrig erfolgte. Die Löschempfehlung korrespondiert mit der Verpflichtung zur Löschung oder Sperrung des Datensatzes gemäß § 10 Abs. 2 Satz 1 Nr. 1 NVerfSchG, da die Speicherung unzulässig war.
Eine Besonderheit der Kategorisierung bestand bei der rechtswidrigen Speicherung von Minderjährigen. Hier war zwischen dem Zeitraum vor und nach Erreichen der Volljährigkeit zu differenzieren. Ergab sich die Rechtswidrigkeit bezogen auf die Speicherung als minderjährige Person allein aufgrund des fehlenden Gewaltbezugs, so konnte die Speicherung weiterer Erkenntnisse nach Erreichen der Volljährigkeit dennoch rechtmäßig erfolgt sein. In diesen Fällen verband die Task Force die Löschempfehlung der Kategorie A (aufgrund der rechtswidrigen Erstspeicherung der oder des Minderjährigen) mit dem Hinweis, dass die Speicherung nach Vollendung des 18. Lebensjahrs als rechtmäßig bewertet wird. Somit wurde in derartigen Fällen ausschließlich die Löschung der Erkenntnisse, die sich auf den Zeitraum vor Vollendung des 18. Lebensjahrs bezogen, empfohlen.

Kategorie B: Wegfall der Erforderlichkeit der Speicherung
Eine Löschempfehlung mit einer Einstufung als Kategorie B beruhte auf der Bewertung der Task Force, dass die Speicherung der personenbezogenen Daten für die Aufgabenerfüllung des Verfassungsschutzes nicht mehr erforderlich war. Gleichzeitig ließ nach Wahrnehmung der Task Force der gegenwärtige Bearbeitungsstand erkennen, dass der jeweilige Fachbereich diese Bewertung nicht teilte. Die Löschempfehlung entspricht der Verpflichtung zur Löschung oder Sperrung ge-

mäß § 10 Abs. 2 Satz 1 Nr. 2 NVerfSchG. Die Rechtmäßigkeit der Erstspeicherung der Daten wurde durch eine Löschempfehlung der Kategorie B nicht in Frage gestellt.

Kategorie C: Vorgezogene Wiedervorlage
Eine Löschempfehlung der Kategorie C erfolgte in Fällen, bei denen die Speicherung nicht länger als erforderlich bewertet wurde und gleichzeitig die Wiedervorlage zeitnah vorgesehen war. Die Empfehlung der Task Force beruhte somit auf der Einschätzung, dass auch der zuständige Fachbereich im Rahmen der Wiedervorlageprüfung zu der Entscheidung gelangen würde, die Daten zu löschen. Es handelte sich daher lediglich um eine vorgezogene Wiedervorlageentscheidung. Dies heißt auch, dass eine Löschempfehlung der Kategorie C ausdrücklich keine Beanstandung der bisherigen Speicherung bedeutet.

Datensätze von 9.004 Personen überprüft

Insgesamt hat die Task Force die Datensätze von 9.004 in der Amtsdatei des Niedersächsischen Verfassungsschutzes gespeicherten Personen überprüft. Als Gesamtarbeitsgruppe hat die Task Force in 39 Sitzungen über 3.059 Personenspeicherungen beraten. Nach der oben beschriebenen Verfahrensweise wurden hiervon 188 Fälle in mehreren Sitzungen vertieft behandelt. Die Task Force empfahl den Verbleib von 5.503 Personenspeicherungen. Dies entspricht einem Anteil von 61,12 Prozent. 1.937 Personenspeicherungen wurden beanstandet und mussten nach Auffassung der Task Force gelöscht werden. Dies entspricht einem Anteil von 21,51 Prozent.
Die Empfehlungen der Task Force sind von der Verfassungsschutzbehörde fast gänzlich umgesetzt worden. Lediglich wenige Fälle (im einstelligen Bereich) wurden nach erneuter, intensiver Überprüfung durch die Behörde weiterhin im Bestand gehalten. Hierbei handelte es sich im Wesentlichen um Vorgänge aus dem Bereich des Ausländerextremismus.
Ich habe die Aktion seinerzeit aus Datenschutzsicht sehr begrüßt und halte das Ergebnis, das die Task Force in Zusammenarbeit mit der Verfassungsschutzbehörde erzielt hat, für einen, unter datenschutzrechtlichen Gesichtspunkten betrachtet, bemerkenswerten und positiven Vorgang.

Mängel seit 2011, fehlende Informationen: Keine Fortschritte bei den TKÜ-Projekten

In meinem XXI. Tätigkeitsbericht für die Jahre 2011 und 2012 habe ich umfassend über einige datenschutzrechtliche und technisch-organisatorische Mängel der niedersächsischen Praxis der polizeilichen Telekommunikationsüberwachung (TKÜ) berichtet. Zahlreiche für eine Mängelbeseitigung erforderliche Maßnahmen sind zwar aufwändig, doch dies ist keine Begründung dafür, dass sie am Ende des Berichtszeitraumes noch immer ausstanden.

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

Erhebliche Defizite

In verschiedenen Analysen, teilweise gemeinsam mit der LfDI Bremen, kritisierte ich die zum Teil erheblichen Defizite bei der Umsetzung der datenschutzrechtlichen Anforderungen. Die bis Ende Mai 2013 zum Teil erst auf Anforderung bei meiner Behörde eingereichten Unterlagen zum Verfahren umfassten 20 Dokumente vor allem zu den für IT-Verfahren üblichen Aspekten

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

Zusätzlich gab es spezifische Dokumente zur Regelung der partiellen Datenlöschung im Kernbereich privater Lebensgestaltung[1] sowie zur Mandantentrennung für verschiedene Polizeibehörden und -dienststellen.

Umfassender Mängelkatalog

In einem vorläufigen Zwischenergebnis nach intensiver kooperativer Prüfung musste ich im Juli 2013 weiterhin eine Reihe von Datenschutzmängeln feststellen. Zum Zeitpunkt der gemeinsamen Prüfung fand der Wirkbetrieb bereits seit neun Monaten statt. Mit Schreiben vom 15. August 2013 setzte ich das LKA Niedersachsen und das Niedersächsische Ministerium für Inneres und Sport von dem aktualisierten Prüfergebnis in Kenntnis.
Bei der zusammenfassenden Betrachtung der zahlreichen Prüfpunkte des vorhandenen TKÜ-Verfahrens wurden in diesem Schreiben sieben gebündelte Problemfelder identifiziert (eine detaillierte Schilderung lag den Schreiben bei, hat in diesem öffentlichen Tätigkeitsbericht aus Sicherheitsgründen jedoch zu unterbleiben):

1. Insbesondere waren die Aussagen zur Risikoanalyse, auch nach Berücksichtigung des Überarbeitungsstandes vom 18. Oktober 2012, noch unvollständig. Es war in der Folge nicht bestimmbar, ob alle erforderlichen technisch-organisatorischen Schutzmaßnahmen gemäß § 7 Abs. 2 Niedersächsisches Datenschutzgesetz (NDSG), insbesondere zur Umsetzung/Überwachung, zur Wartung/Fernwartung, zum Datenexport, zur Netzsicherheit und bei der Verknüpfung mit weiteren Datenverarbeitungsverfahren getroffen worden waren. Die Risikoanalyse und eine Bewertung von Gefahren im Kontext mit dem Schutzbedarf sollte bis 31. Dezember 2014 abgeschlossen werden. Sie lag meinem Haus bis zum Ende des Berichtszeitraumes nicht vor.
2. Nach meinen Erkenntnissen ist die erforderliche Mandantenfähigkeit des Verfahrens im datenschutzrechtlichen Sinne nicht erwiesen. Die Beschreibung in den Dokumenten hierzu lässt erkennen, dass es einer strukturellen Nachbesserung bedarf. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zur Umsetzung einer datenschutzkonformen Implementierung und Ausgestaltung der Mandantenfähigkeit von IT-Verfahren eine Orientierungshilfe[2] veröffentlicht, die dem LKA Niedersachsen sehr frühzeitig zur Kenntnis gegeben worden war. Danach lässt sich in fünf Prüfschritten feststellen, wann eine ausreichende Trennung im Verfahren erfüllt ist und wann es damit dem Zweckbindungsgebot und Trennungsgebot, dem Schutzziel der Vertraulichkeit und der Nichtverkettbarkeit entspricht.

---

1 Der Kernbereichsschutz gem. § 100 a Abs. 4 Strafprozessordnung (StPO) fußt auf der vom Bundesverfassungsgericht in mehreren Entscheidungen geforderten Differenzierung zwischen Daten, die unter normenklaren Bedingungen ermittelt und verarbeitet werden dürfen, und Daten, die dem unantastbaren Kernbereich privater Lebensumstände zuzuordnen sind. Letztere unterliegen dem absoluten, also ausnahmslosen Schutz vor staatlichen Eingriffen, dürfen folglich nicht erhoben werden und unterliegen einem Beweisverwertungsverbot. Werden sie im Zuge eines mitgeschnittenen Datenstreams oder eines Telefonates dennoch unvermeidbar erhoben, sind sie unverzüglich nach Identifizierung als solche rückstandsfrei zu löschen. Vgl.
BVerfG, Urteil vom 16. Januar 1957, Az. 1 BvR 253/56, BVerfGE 6, 32 41;
BVerfG, Beschluss vom 14. September 1989, Az. 2 BvR 1062/87, BVerfGE 80, 367 bis 383;
BVerfG, Beschluss vom 13. Juni 2007, Az. 1 BvR 1783/05, BVerfGE 119, 1 bis 59.

2 „Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit – des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder – Version 1.0" vom 11. Oktober 2012 – Quelle: http://www.lfd.niedersachsen.de > Menü > Navigation > Technik und Organisation > Orientierungshilfen und Handlungsempfehlungen > Mandantenfähigkeit; Deeplinks: http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=31646&article_id=109520&_psmand=48 oder http://www.lfd.niedersachsen.de/download/71664/Orientierungshilfe_Mandantenfaehigkeit_AK_Technik_.pdf

3. Das Rechte-Rollen-Konzept ist insgesamt zu vervollständigen. Hier fehlen einige entscheidende Differenzierungen sowie die Einhaltung des Vier- oder Mehr-Augen-Prinzips in der Administration.
4. Die Protokollierung der Datenverarbeitungsschritte ist um festgestellte fehlende Komponenten und Maßnahmen zu ergänzen.
5. Die Dokumentenlage ist – trotz des bereits vorhandenen Umfangs – gleichwohl in Teilen lückenhaft, so dass weder der gesicherte und rechtssichere Betrieb, noch eine Revisionssicherheit gewährleistet werden können. Angesichts des in diesem Verfahren sehr hohen und sensiblen Schutzbedarfes und der vorliegenden Gefährdungen und Risiken ist es von essenzieller Bedeutung, dass zu jeder Zeit und in einem ständig fortgeschriebenen Zustand eine vollständige Dokumentation vorliegt. Diese dient der sicheren Orientierung für den verantwortungsvollen Betrieb und für eine erforderliche Revision.
6. Aufgrund des festgestellten sehr hohen Schutzbedarfes ist die Verschlüsselung der Inhalts- und der Verkehrsdaten vorzunehmen.
7. Die Fernwartung ist nur mit besonderen, der Schutzstufe „sehr hoch“ angemessenen Sicherheitsmaßnahmen zulässig. Der Nachweis zu den Maßnahmen ist noch zu erbringen.

44 Mängelpunkte, ein Ministergespräch, null Erfolg

Von den zahlreichen erörterten Fragen blieben nach den Gesprächen zwischen November 2011 und Juli 2013 insgesamt 44 einzelne Punkte übrig, die als offen oder unerledigt zu bewerten sind oder einen Dissens in der Bewertung (belastet, kritisch oder hochkritisch) aufweisen. Aufgrund der Gesamtbewertung hielt ich daher das Verfahren im Wirkbetrieb zum damaligen Zeitpunkt für unzulässig. Ein entsprechendes Schreiben an das LKA Niedersachsen und an das Niedersächsische Ministerium für Inneres und Sport, das mit inhaltlicher Entsprechung auch die LfDI Bremen zeitgleich an die Polizei Bremen richtete, erläuterte mein Amtsvorgänger dem niedersächsischen Innenminister am 17. September 2013 in einem persönlichen Gespräch.
Zum Ende des Berichtszeitraumes im Dezember 2014 standen die geforderten Nachbesserungen noch immer aus. Insbesondere ist nicht verständlich, warum die für die Angemessenheit der Schutzmaßnahmen so grundlegende Risikobewertung noch nicht abgeschlossen vorgelegt worden ist. Die fortdauernden Mängel führten auch zu der in meinem Haus gezogenen Schlussfolgerung, dass vor einem Kooperationsbetrieb mit den Polizeien anderer Länder die Planungen sowie die unterschriftsfähigen Unterlagen zunächst derartige Mängel ausschließen müssen, damit sich diese nicht zusätzlich auf die anderen Länder ausdehnen. Ich sehe der Kooperation daher weiterhin mit der gebotenen Aufmerksamkeit entgegen.

Was wird aus dem geplanten RDZ-TKÜ der Küstenländer?

Parallel zum Wirkbetrieb dieses bestehenden TKÜ-Verfahrens liefen die 2011 begonnenen Planungen für ein Kooperationsprojekt „Rechen- und Dienstleistungszentrum Telekommunikationsüberwachung der Polizei im Verbund der norddeutschen Küstenländer (RDZ-TKÜ)“ zunächst weiter. Zu dieser Planung der Länder Bremen, Hamburg,

Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein und die beratende Begleitung meiner Behörde hatte ich ebenfalls im letzten Tätigkeitsbericht eine ausführliche Stellungnahme abgegeben.
Bis zum Mai 2013 wurde das Thema wiederholt auf Fachebene der Rechts- und Technikreferate der Datenschutzbeauftragten der beteiligten Bundesländer erörtert, insbesondere vor dem Hintergrund der Erfahrungen mit dem Wirkbetrieb des LKA Niedersachsen. Zeitweise wurden die Gespräche gemeinsam mit der länderübergreifenden polizeilichen Projektgruppe geführt, die bereits 2011 unter Federführung des LKA Niedersachsen konstituiert worden war. Dabei lag ein besonderes Augenmerk auf den teils abweichenden Bewertungen der Polizei zu den von mir im Konsens mit den übrigen Landesdatenschutzbeauftragten (LfD) aufgestellten Anforderungen. Es besteht auch Einigkeit mit den vier anderen LfD darin, dass Erfahrungen mit dem Hersteller und Dienstleister der TKÜ-Software bezüglich nicht geleisteter oder leistbarer Anpassungen an datenschutzrechtliche Anforderungen auch erhebliche Auswirkungen auf künftige Ausschreibungen und Leistungsbeschreibungen haben müssen; dies umso mehr, als grundlegende Mängel oder Schwachstellen eine flächendeckende Wirkung auf Betroffene in fünf Bundesländern haben würden. Insofern bieten die Optimierungsanforderungen gleichzeitig einen Ausblick auf die Anforderungen an das Kooperationsprojekt.

Keine Informationen über Stand des Projekts

Im April 2014 erreichte meine Behörde die Information aus der Projektgruppe RDZ-TKÜ-Verbund, dass der Hamburger Senat beschlossen habe, nicht mehr am Kooperationsprojekt der fünf Küstenländer für ein gemeinsames TKÜ-Zentrum teilzunehmen. Es verblieben somit noch vier Länder als Kooperationspartner. Bei diesen, so hieß es weiter, stünde derzeit (April 2014) auf politischer Ebene der Innenminister eine Entscheidung aus, ob weiter an einem RDZ festgehalten werden solle. Bis zur Entscheidung würden im Kooperationsprojekt alle weiteren Tätigkeiten ruhen. Die Kooperation zwischen Bremen und Niedersachsen sei davon jedoch unberührt. Über den Fortgang oder ein Ergebnis dieses Entscheidungsprozesses wurden bis zum Ende des Berichtszeitraumes weder ich, noch die Datenschutzbeauftragten der anderen Länder informiert.

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

2. Datenschutz in Kommunen

Neues Bundesmeldegesetz: Datenschutzbeauftragte bei Novellierung niedersächsischer Vorschriften beteiligt

Im Zuge der Föderalismusreform I wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Bundestag und Bundesrat haben das Gesetz zur Fortentwicklung des Meldewesens mit einem Bundesmeldegesetz als Kernstück Anfang 2013 beschlossen. Das Gesetz zur Änderung des Gesetzes zur Fortentwicklung des Meldewesens vom 3. Juli 2014 enthält einige wenige Änderungen des Bundesmeldegesetzes, das nunmehr am 1. November 2015 in Kraft treten wird. Mit diesem Gesetz werden die bis dahin geltenden Meldegesetze der einzelnen Bundesländer ersetzt; erstmals wird es dann bundesweit einheitliche und unmittelbar geltende melderechtliche Vorschriften geben.

Als neue Regelungen sind besonders hervorzuheben:

Melderegisterauskünfte für gewerbliche Zwecke:
Bei entsprechenden Anfragen ist künftig der Zweck der Anfrage anzugeben. Die Melderegisterauskunft darf ausschließlich zum angegebenen Zweck verwandt werden.

Melderegisterauskünfte für Zwecke der Werbung und des Adresshandels:
Entsprechende Auskünfte sind künftig nur noch mit Einwilligung der betroffenen Person möglich.

Online-Zugriff durch Sicherheitsbehörden:
Sicherheitsbehörden und weitere, durch Rechtsvorschriften zu bestimmende Behörden erhalten rund um die Uhr länderübergreifend einen Online-Zugriff auf die Meldedaten.

Vereinfachung des Hotelmeldeverfahrens und Verfahrens bei Aufenthalten in Krankenhäusern, Heimen und ähnlichen Einrichtungen.

Gemeinsam
IT gestalten.

IT.Niedersachsen

Anlage zum Antrag auf Zugang zum Melderegisterdatenspiegel:

Formular: Nutzerdaten der Administratorin/des Administrators für die Registrierung im Melderegisterdatenspiegel Niedersachsen

☐ Herr ☐ Frau

Vorname

Name

Emailadresse

Name der Dienststelle

Straße und Hausnummer der Dienststelle

PLZ und Ort der Dienststelle

Wiedereinführung der Mitwirkungspflicht des Vermieters
bei der Anmeldung von Mietern zur Vermeidung von Scheinanmeldungen.

Evaluation der neuen Regelungen durch die Bundesregierung auf wissenschaftlicher Grundlage und Berichterstattung an Bundestag und Bundesrat vier Jahre nach Inkrafttreten des Gesetzes.

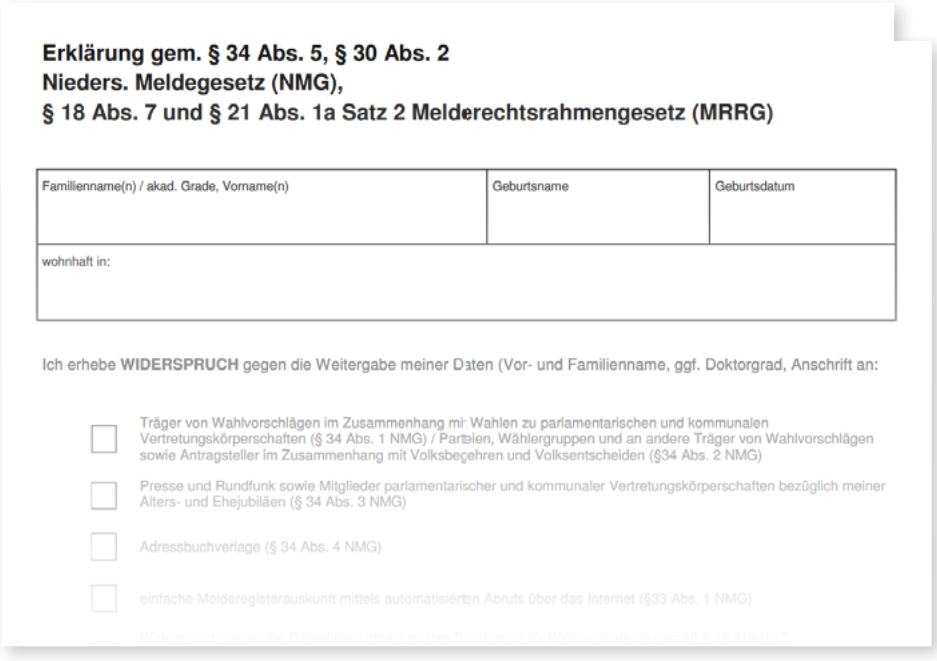
Niedersachsen richtet Melderegisterdatenspiegel ein
Mit Inkrafttreten des Bundesmeldegesetzes wird auch für Niedersachsen die Verpflichtung bestehen, Melderegisterdaten zum automatisierten Abruf für die Sicherheitsbehörden zu jeder Zeit bereitzuhalten. Da dieses aus den kommunalen niedersächsischen Melderegistern nicht effizient erfüllt werden könnte, übernimmt das Land Niedersachsen diese Aufgabe künftig selbst und wird den Melderegisterdatenspiegel Niedersachsen (MiN) einrichten, der die Abrufmöglichkeit sicherstellen wird.
Für die Errichtung des MiN, die Durchführung von Systemtests und die Befüllung mit Melderegisterdaten mussten die rechtlichen Regelungen des Niedersächsischen Meldegesetzes (NMG) als auch der Niedersächsischen Meldedatenübermittlungsverordnung (NMeldDÜV) überarbeitet werden. In beide Verfahren war meine Behörde eingebunden. Das Gesetz zur Änderung des NMG trat am 30. Juli 2014 in Kraft, die Verordnung zur Änderung der Meldedatenübermittlungsverordnung am 24. September 2014.

Beteiligung der Datenschutzbeauftragten zugesagt
Für das neue Bundesmeldegesetz wird seitens des Niedersächsischen Ministeriums für Inneres und Sport neues ausführendes Landesrecht zu erstellen sein. Eine weitere Beteiligung der Landesbeauftragten für den Datenschutz wurde bereits angekündigt.

Weitergabe von Meldedaten innerhalb der Gemeinde: Nur zur Erfüllung von Aufgaben erlaubt

Auch im Berichtszeitraum erreichten mich Anfragen von verschiedenen Stellen der Gemeinden wie Stadtbücherei, Feuerwehr, Rechnungsprüfungsamt oder Kulturbüro, ob die im Melderegister der örtlichen Meldebehörde gespeicherten Daten von dieser an andere Stellen innerhalb der Gemeinde weitergeben werden dürfen, wenn diese danach fragen. Ebenso erreichten mich Eingaben von Bürgern, die wissen wollten, warum der Ortsbürgermeister bzw. Ortsvorsteher Meldedaten erhalten dürfe.

Neben dem Einwohnermeldeamt, also der Meldebehörde, benötigen häufig auch andere Stellen innerhalb der Gemeinde Daten aus dem Melderegister, um ihre Aufgaben erfüllen zu können. Das Vorhandensein einer Vielzahl personenbezogener Daten im Melderegister weckt jedoch mitunter die Begehrlichkeit bei weiteren Stellen innerhalb einer Gemeinde, die Meldedaten für verschiedenste Zwecke nutzen zu wollen. Jedoch sollte jede Stelle vor einer Anfrage an die Meldebehörde immer prüfen, ob eine Datenweitergabe im Rahmen der melde- und datenschutzrechtlichen Vorschriften überhaupt möglich und zulässig ist.
Nach § 29 Abs. 6 des Niedersächsischen Meldegesetzes (NMG) dürfen innerhalb einer Gemeinde sämtliche der in § 22 Abs. 1 NMG aufgeführten Daten und Hinweise (unter anderem Familienname, Vorname, gegenwärtige und frühere Anschrift) sowie das Ordnungsmerkmal durch die Meldebehörde bekanntgegeben werden. Bei der Bekanntgabe der Daten innerhalb der Gemeinde handelt es sich nicht um eine Datenübermittlung, sondern um eine Datennutzung. Das bedeutet, dass eine Weiterleitung von Meldedaten an andere Stellen innerhalb einer Gemeinde sowohl melderechtlich als auch datenschutzrechtlich zulässig ist, soweit die Daten für die Erfüllung der gesetzlichen Aufgaben der Meldebehörde oder des Empfängers erforderlich sind.



Erklärung gem. § 34 Abs. 5, § 30 Abs. 2 Nieders. Meldegesetz (NMG), § 18 Abs. 7 und § 21 Abs. 1a Satz 2 Melderechtsrahmengesetz (MRRG)

Familienname(n) / akad. Grade, Vorname(n)	Geburtsname	Geburtsdatum
wohnhaft in:		

Ich erhebe **WIDERSPRUCH** gegen die Weitergabe meiner Daten (Vor- und Familienname, ggf. Doktorgrad, Anschrift an:

- ☐ Träger von Wahlvorschlägen im Zusammenhang mit Wahlen zu parlamentarischen und kommunalen Vertretungskörperschaften (§ 34 Abs. 1 NMG) / Parteien, Wählergruppen und an andere Träger von Wahlvorschlägen sowie Antragsteller im Zusammenhang mit Volksbegehren und Volksentscheiden (§34 Abs. 2 NMG)
- ☐ Presse und Rundfunk sowie Mitglieder parlamentarischer und kommunaler Vertretungskörperschaften bezüglich meiner Alters- und Ehejubiläen (§ 34 Abs. 3 NMG)
- ☐ Adressbuchverlage (§ 34 Abs. 4 NMG)
- ☐ einfache Melderegisterauskunft mittels automatisierten Abrufs über das Internet (§33 Abs. 1 NMG)

Über die Feststellung der Erforderlichkeit hat die anfordernde Stelle jeweils im Einzelfall in eigener Verantwortung zu entscheiden.

Keine Datenweitergabe für Werbe- und Informationszwecke

Auch wenn eine Prüfung der Erforderlichkeit jeweils im Einzelfall vorzunehmen ist, lässt sich doch grundsätzlich annehmen, dass die Datenweitergabe an Stellen innerhalb der Gemeinde voraussichtlich dann nicht erforderlich sein wird, wenn es um die Nutzung der Daten für Marketingzwecke geht oder die Daten für den Versand von Informationen an bestimmte Personenkreise wie Neubürger, Rentner, Familien mit Kindern und Kulturinteressierte benötigt werden. Denn diesen Stellen stehen auch andere datenschutzfreundlichere Möglichkeiten zur Verfügung, sich und ihre Angebote bekannt zu machen, zum Beispiel über die Tagespresse, Flyer oder Aushänge.

Zur Wahrnehmung des Ehrenamtes oder repräsentativer Aufgaben im Einzelfall zulässig

Nur wenn Stellen ihre gesetzlichen Aufgaben mangels Verfügbarkeit der Melderegisterdaten nicht wahrnehmen können, kann im Einzelfall eine Erforderlichkeit angenommen werden. Die Abwehr von Gefahren durch Brände (abwehrender und vorbeugender Brandschutz) obliegt den Gemeinden und Landkreisen als Aufgabe des eigenen Wirkungskreises gemäß § 1 Abs. 1 und Abs. 2 des Niedersächsischen Brandschutzgesetzes. Würden sich in einer Gemeinde oder einem Ortsteil beispielsweise nicht genug Freiwillige für die Feuerwehr engagieren und sich auch nach einer Werbung mittels Postwurfsendungen, Flyern oder Aushängen keine neuen Mitglieder für die Feuerwehr finden lassen, könnte die Gemeinde in so einem speziellen Einzelfall ihrer gesetzlichen Brandschutzpflicht, zu der auch die Aufstellung von Feuerwehren gehört, nicht nachkommen. Die Übermittlung von Meldedaten von Einwohnern eines bestimmten Ortsteils oder einer bestimmten Altersgruppe an die Feuerwehr, die in aller Regel organisatorisch dem Ordnungsamt angegliedert ist, wäre dann vermutlich erforderlich, um potentiellen Feuerwehrnachwuchs mit einem speziellen Informationsschreiben anzusprechen.
Organe der Gemeinde wie zum Beispiel Ortsbürgermeister oder Ortsvorsteher nehmen bestimmte Aufgaben der Gemeinde im Rahmen ihrer Funktion wahr. Hierunter fallen auch Gratulationen zu Alters- und Ehejubiläen. Für die Wahrnehmung dieser Aufgaben bedürfen sie der Kenntnis bestimmter personenbezogener Daten, die ihnen die Meldestelle zuleiten darf. Diese für einen konkreten Zweck erhaltenen personenbezogenen Meldedaten dürfen dann jedoch nicht für weitere Aufgaben und Zwecke oder gar für private Zwecke wie die Weitergabe an Parteigenossen genutzt werden.

Neues Bundesmeldegesetz ab dem 1. November 2015 in Kraft

Auch nach der mit Inkrafttreten des Bundesmeldegesetzes (BMG) geltenden Vorschrift des § 37 Abs. 1 BMG dürfen Meldedaten in einem mit dem derzeitigen § 29 Abs. 6 NMG vergleichbaren Umfang innerhalb der Verwaltungseinheit, der die Meldebehörde angehört, weitergegeben werden, soweit die Daten nach § 34 Abs. 1 BMG erforderlich sind.

Meldedatenabgleich für Rundfunkbeiträge: Gerichte bestätigen Datenübermittlung

Mit der Neufassung des Rundfunkstaatsvertrages (RStV) endete die Bindung der Gebührenpflicht für Rundfunknutzer an das Bereithalten von Rundfunkempfangsgeräten. Als wesentliche Neuerung trat zum 1. Januar 2013 eine Beitragspflicht für Wohnungsinhaber im privaten Bereich und für Betriebsstätteninhaber im nicht-privaten Bereich in Kraft. Die von den Landesrundfunkanstalten eingerichtete GEZ wurde zeitgleich in „ARD ZDF Deutschlandradio Beitragsservice" umbenannt.

Nach Artikel 1 des Niedersächsischen Gesetzes zum 15. Rundfunkänderungsstaatsvertrages (RÄndStV) vom 29. Juni 2011 i. V. m. § 2 Abs. 1 Rundfunkbeitragsstaatsvertrag (RBStV) ist im privaten Bereich nun für jede Wohnung von deren Inhaber (Beitragsschuldner) ein Rundfunkbeitrag zu entrichten. Gemäß § 2 Abs. 2 RBStV ist Inhaber unter anderem jede volljährige Person, die die Wohnung selbst bewohnt; als Inhaber wird weiterhin jede Person vermutet, die dort nach dem Melderecht gemeldet ist.

Einmaliger Meldedatenabgleich ermöglicht Bestandserfassung der Wohnungen

Um einen einmaligen Abgleich zum Zwecke der Bestands- und Ersterfassung im Rahmen des ab 2013 geänderten Rundfunkbeitragsgebührenmodells zu ermöglichen, hat jede Meldebehörde in Deutschland nach § 14 Abs. 9 RBStV automatisiert in standardisierter Form acht Datenfelder innerhalb von längstens zwei Jahren ab Inkrafttreten des RBStV (das heißt bis zum 31. Dezember 2015) an den ARD ZDF Deutschlandradio Beitragsservice für alle volljährigen Personen zu übermitteln, die zu dem Stichtag 3. März 2013 bei ihr gemeldet waren:

- Name, Vorname,
- frühere Namen,
- Doktorgrad,
- Familienstand,
- Tag der Geburt,
- aktuelle und vorherige Anmeldungen der Haupt- und Nebenwohnungen und
- Tag des Einzugs.

Nicht alle Einwände der Datenschutzbeauftragten berücksichtigt

In den Jahren 2013 und 2014 erreichten mich zahlreiche Eingaben von Bürgern, zumeist sogar in Form eines aus dem Internet herunterladbaren Musterschreibens, mit dem diese sich gegen die Weitergabe ihrer im Melderegister gespeicherten Daten an die Landesrundfunkanstalt bzw. den ARD ZDF Deutschlandradio Beitragsservice wandten. Die Voraussetzungen für den einmaligen Meldedatenabgleich sind gesetzlich fixiert und wurden im Vorfeld intensiv – unter anderem mit den Landesbeauftragten für den Datenschutz – diskutiert. Seitens der Landesbeauftragten wurden zwar Einwände gegen den Meldedatenabgleich erhoben – zum Beispiel, dass dieser zusätzlich zu der ohnehin regelmäßigen Datenübermittlung bei An- und Abmeldungen sowie Geburten und Todesfällen erfolge – , jedoch fanden nicht alle Einwände und Vorschläge der Datenschutzbeauftragten ihren Niederschlag im Rundfunkbeitragsstaatsvertrag. Vom Gesetzgeber ist vielmehr ein flächendeckender einheitlicher Abgleich zwischen Meldedaten und Beitragspflichtigen gewollt. Die Verarbeitung der beim Meldedatenabgleich übermittelten Angaben unterliegt dabei einer strengen datenschutzrechtlichen Zweckbindung. Die einfachgesetzlichen Regelungen des RBStV lassen somit die Datenübermittlung zu. Dieses wurde den Bürgern mitgeteilt.

OVG Lüneburg bestätigt Zulässigkeit des Meldedatenabgleichs

Mit Urteil vom 10. September 2013 (Az.: 4 ME 204/13) befand auch das Oberverwaltungsgericht Lüneburg die Datenübermittlung an den ARD ZDF Deutschlandradio Beitragsservice für rechtens. Das Gericht konnte keinen unzulässigen Eingriff in das Recht auf informationelle Selbstbestimmung feststellen. Auch andere deutsche Gerichte vertraten inzwischen die gleiche Auffassung.

ARD ZDF Deutschlandradio
BEITRAGSSERVICE

Reisegewerbekarte: Keine Datenübermittlung an die Kammern

Im Gewerberecht gibt es keine Datenübermittlungsbefugnisse der Gewerbeämter bei der Beantragung eines Reisegewerbes.

Die gesetzlichen Regelungen für ein Reisegewerbe finden sich in den §§ 55 ff unter Titel III der Gewerbeordnung (GewO). Soweit keine reisegewerbekartenfreie Tätigkeit vorliegt, bedarf es zum Betrieb eines Reisegewerbes gemäß § 55 Abs. 2 GewO der Erlaubnis. Diese Erlaubnis wird in Form einer Reisegewerbekarte erteilt und von der jeweils zuständigen Behörde ausgestellt.
Für das stehende Gewerbe darf die zuständige Behörde gemäß § 14 Abs. 8 GewO Daten aus der Gewerbeanzeige unter anderem regelmäßig übermitteln an

- die Industrie- und Handelskammer (IHK) zur Wahrnehmung der in den §§ 1, 3 und 5 des Gesetzes zur vorläufigen Regelung des Rechts der IHK genannten sowie der nach § 1 Abs. 4 desselben Gesetzes übertragenen Aufgaben (zum Beispiel Erhebung von Grundbeiträgen und Umlagen von Gewerbebetrieben),
- die Handwerkskammer zur Wahrnehmung der in § 91 der Handwerksordnung genannten, insbesondere der ihr durch die §§ 6, 19 und 28 der Handwerksordnung zugewiesenen und sonstiger durch Gesetz übertragener Aufgaben (zum Beispiel Auskunfterteilung aus der Handwerksrolle bei Vorliegen eines berechtigten Interesses).

MW folgt der Bitte um Sensibilisierung

Diese Datenübermittlungsbefugnis findet allerdings ausschließlich auf das stehende Gewerbe, nicht aber auf das Reisegewerbe Anwendung. Die Gewerbeordnung enthält keine Rechtsvorschrift, die im Rahmen der Reisegewerbekartenausstellung eine Datenübermittlung von den Gewerbeämtern an die Kammern vorsieht. Eine solche Datenübermittlung ist damit in jedem Fall unzulässig.
Aufgrund aktueller Anfragen wurde die unzulässige Datenübermittlung an Kammern im Rahmen der Reisegewerbekartenausstellung auch im Bund-Länder-Ausschuss – Gewerberecht thematisiert. Die Feststellung der Unzulässigkeit wird von dort und auch vom Niedersächsischen Ministerium für Wirtschaft, Arbeit und Verkehr (MW) geteilt. Das MW hat im Juli 2014 die niedersächsischen Gewerbeämter auf meine Anregung hin noch einmal sensibilisiert und entsprechend in Kenntnis gesetzt.

Das Niedersächsische Hunderegister: Und noch eine staatliche Datenbank

Mit der Neufassung des Niedersächsischen Gesetzes über das Halten von Hunden (NHundG) vom 26. Mai 2011 wurde das Niedersächsische Hunderegister ins Leben gerufen. Im Rahmen der Anhörung hatte ich im September 2010 zu dem seinerzeitigen Gesetzentwurf, insbesondere zu den Regelungen hinsichtlich des Hunderegisters, Stellung genommen und angeregt, vor Einführung dieses Registers noch einmal zu prüfen, ob nicht stattdessen auf bestehende Register zurückgegriffen werden könne. Zudem hatte ich darauf hingewiesen, dass im Hinblick auf das Gebot der Datenvermeidung und Datensparsamkeit bereits bei der Entwicklung und Auswahl von Datenverarbeitungssystemen darauf hinzuwirken sei, dass keine oder möglichst wenige personenbezogene Daten verarbeitet werden.

Nach den nunmehr in Kraft getretenen gesetzlichen Bestimmungen des NHundG soll das Register der Identifizierung eines Hundes dienen sowie der Ermittlung der Hundehalterin oder des Hundehalters und der Gewinnung von Erkenntnissen über die Gefährlichkeit von Hunden in Abhängigkeit von Rasse, Geschlecht und Alter. In dem Register werden nach Maßgabe des § 6 NHundG Angaben der Hundehalter gespeichert. Diese sind in Niedersachsen seit dem 1. Juli 2013 gesetzlich dazu verpflichtet, vor Vollendung des 7. Lebensmonats ihres Hundes und bei älteren Hunden innerhalb eines Monats ab Beginn der Hundehaltung ihren Hund gegenüber dem zentralen Register zu melden.
Folgende Angaben der Hundebesitzer werden in dem zentralen Register gespeichert:

1. Name, bei natürlichen Personen auch Vorname, Geburtstag, Geburtsort,
2. Anschrift,
3. Geschlecht und Geburtsdatum des Hundes,
4. Rassezugehörigkeit des Hundes oder, soweit feststellbar, die Angabe der Kreuzung und
5. Kennnummer des Hundes (Transponder gem. § 4 Satz 1 NHundG).

Zudem sind folgende Änderungsmitteilungen gegenüber der registerführenden Stelle anzugeben:

- Aufgabe des Haltens des Hundes,
- Abhandenkommen und Tod des Hundes sowie
- Änderungen der Anschrift.

Dem Niedersächsischen Ministerium für Ernährung, Landwirtschaft und Verbraucherschutz (ML) obliegt als zuständigem Fachministerium das Führen des Registers. Im Auftrag des ML wird das Hunderegister Niedersachsen von der Firma GovConnect GmbH (vormals: Kommunale Systemhaus Niedersachsen GmbH) als Beliehene betrieben. Die Rechts- und Fachaufsicht über das zentrale Hunderegister führt das ML. Auf das Hunderegister finden die Regelungen des Niedersächsischen Datenschutzgesetzes (NDSG) Anwendung. Das ML sowie der extern bestellte Datenschutzbeauftragte für das Hunderegister bestätigten, dass das Register den datenschutzrechtlichen Anforderungen, insbesondere den technisch-organisatorischen Anforderungen und dem IT-Sicherheitskonzept entspricht.

Rechnung statt Gebühr

Im Rahmen der Registrierung erhebt die GovConect GmbH für die Entgegennahme und Bearbeitung einer Mitteilung nach § 6 Abs. 1 NHundG eine einmalige Gebühr, die ausschließlich der Unterhaltung des Registers dient und dem Äquivalenzprinzip unterliegt. Die Gebühr richtet sich nach der Niedersächsischen Allgemeinen Gebührenordnung (Nds. AllGO). Auch Änderungen nach § 6 Abs. 2 NHundG sind

mit dieser Gebühr bereits abgegolten. Die Höhe der Gebühr richtet sich nach dem Aufwand der registerführenden Stelle. Da eine Online-Registrierung über die Webseite https://www.hunderegister-nds.de einen geringeren Aufwand für die registerführende Stelle verursacht als eine schriftliche oder telefonische Anmeldung, erhebt diese hierfür eine geringere Gebühr von den Hundehalterinnen und -haltern als für eine schriftliche oder telefonische Anmeldung.
Mit Urteil vom 17. November 2014 stellte das Verwaltungsgericht Hannover fest, dass die GovConnect GmbH nicht befugt sei, Gebührenbescheide zu erlassen. Das Unternehmen sah daraufhin zunächst von der Versendung weiterer Gebührenbescheide ab. Zwischenzeitlich ist es dazu übergegangen, Mitteilungen über die zu zahlenden Gebühren als Rechnung zu versenden. Ungeachtet der Art der Gebührenfestsetzung bleibt die Pflicht zur Mitteilung an das Hunderegister bestehen. Hundebesitzer können lediglich frei entscheiden, auf welche Weise sie die Anmeldung ihres Hundes vornehmen wollen. Eine Nutzung der Daten, die bereits im Rahmen der Hundesteueranmeldung von der jeweils zuständigen Kommune erhoben worden sind, ist datenschutzrechtlich nicht zulässig. In diesem Zusammenhang sei darauf hingewiesen, dass sich Art und Umfang der Datenerhebung für die Hundesteueranmeldung in den Kommunen unterscheiden, da die Festsetzung der Hundesteuer von Kommune zu Kommune unterschiedlich ist und durch das jeweilige Ortsrecht wie zum Beispiel Hundesteuersatzungen geregelt wird.

Keine Verwendung für andere Zwecke

Aber auch die Daten, die im Hunderegister gespeichert sind, sind an ihren Erhebungszweck gebunden und dürfen nicht für andere Zwecke verwendet werden. Den Gemeinden obliegt die Überwachung der Einhaltung der §§ 2–6 und 14 NHundG. Die Landkreise und kreisfreien Städte überwachen als Fachbehörden die Einhaltung der übrigen Vorschriften des NHundG. Im Rahmen ihrer Aufgabenerfüllung nach dem Hundegesetz können die Fachbehörden und Gemeinden Auskunft aus dem zentralen Register einholen. Aufgrund der Gebührenfestsetzung ist es erforderlich, dass die gesetzlich vorgeschriebenen Aufbewahrungsfristen beachtet werden. Eine Löschung von Angaben im Halterkonto ist daher nur bedingt möglich. Angaben oder Belege (Rechnungen), die aufgrund gesetzlich vorgeschriebener Fristen zehn Jahre aufbewahrt und erst nach Ablauf dieser Frist gelöscht werden dürfen, können im Halterkonto lediglich gesperrt, nicht aber vor Ende der Aufbewahrungsfrist endgültig gelöscht werden. Nach Ablauf von zehn Jahren erfolgt eine automatisierte Löschung der Daten.
Soweit Hundehalterinnen und -halter Fragen zum Verfahren haben, können sie sich jederzeit auch direkt an den Datenschutzbeauftragten für das Hunderegister wenden:
Zweckverband Kommunale Datenverarbeitung Oldenburg (KDO), Elsässer Straße 66, 26121 Oldenburg, Telefon 0441 9714-159, E-Mail: datenschutzbeauftragter@hunderegister-nds.de.

Weitere Informationen: http://www.ml.niedersachsen.de/portal/live.php?navigation_id=1810&article_id=93854&_psmand=7

3. Schule

Webbasierte Lernplattformen und Whiteboards: Eindeutige Rahmenbedingungen für Schulen überfällig

Die Schulen setzen immer mehr auf webgestützte Wissensvermittlung und elektronische Kommunikationsmöglichkeiten zwischen Schülerinnen und Schülern und ihren Lehrkräften. Zu diesen Zwecken werden zunehmend onlinebasierte Verfahren, so genannte Lern-, Kommunikations- und Arbeitsplattformen, eingesetzt, bei denen auch personenbezogene Daten der Schülerinnen, Schüler und der Lehrkräfte verarbeitet werden. Daneben nimmt auch in der Schulverwaltung die elektronische Datenverarbeitung immer mehr zu. Diese Verfahren müssen datenschutzrechtliche (Mindest-)Kriterien erfüllen.

Ich habe in mehreren Schreiben und Gesprächen das Niedersächsische Kultusministerium auf die datenschutzrechtliche Problematik bei der Einführung von Lernplattformen hingewiesen und empfohlen, einheitliche und eindeutige Rahmenbedingungen für die Nutzung dieser Verfahren festzulegen. Dies ist leider bislang nicht geschehen.
Weil diese Thematik in allen Bundesländern aktuell ist und dort ebenfalls sehr viele Anfragen von Schulen zu diesem Thema eingegangen sind, haben die Datenschutzbeauftragten von Bund und Ländern über ihren Arbeitskreis Datenschutz und Bildung eine Orientierungshilfe für Online-Lernplattformen im Schulunterricht erarbeitet, die sich momentan noch in der Abstimmung befindet. Sobald sie fertiggestellt ist, werde ich sie auf meiner Homepage einstellen, um sie allen Schulen zugänglich zu machen. Darüber hinaus ist in meinem Technikreferat derzeit noch eine Orientierungshilfe mit Checkliste „Datenschutz für IT-Systeme und -Verfahren in Schulen“ in der Entwicklung, die derzeit aus Kapazitätsgründen noch nicht finalisiert werden konnte. Es wird hier noch eine Abstimmung mit der zuvor genannten Orientierungshilfe für Online-Lernplattformen im Schulunterricht angestrebt.

Orientierungshilfe für Online-Lernplattformen und IT-Systeme und -Verfahren in Schulen geplant

Viele Anfragen von Lehrkräften und Schulleitungen

Viele Schulen bieten inzwischen sogenannte Laptop- und iPad-Klassen an und arbeiten mit digitalen Tafeln wie Whiteboards oder Smartboards. Trotzdem herrschen an fast allen Schulen große Unsicherheit und Unkenntnis im Umgang mit personenbezogenen Daten, wie ich den ständigen Anfragen und Telefonaten aus dem Schulbereich entnehmen muss. Meine Empfehlung, den Schulen grundlegende Informationen in Form von Merkblättern, Orientierungshilfen, Muster-Verfahrensbeschreibungen zur Verfügung zu stellen, wurde

bereits teilweise umgesetzt. Dies unterstützt aber nur bedingt die Schulleitungen, die mit den wachsenden Anforderungen, die eine immer stärker auf elektronische Datenverarbeitung gestützte Schulverwaltung mit sich bringt, zeitlich und inhaltlich überfordert sind. Auch hier wäre es wünschenswert, wenn den Schulen einheitliche und eindeutige Rahmenbedingungen für den Einsatz digitaler Medien zur Verfügung gestellt würden.

Leider keine dienstlichen Geräte und keine Trainings

Ein weiteres großes Problem besteht darin, dass den Lehrkräften keine dienstlichen Geräte zur Verfügung gestellt werden, so dass sie „gezwungenermaßen" auf ihre eigenen Geräte zurückgreifen. Dabei wird übersehen, dass weiterhin die Schule datenverarbeitende Stelle im Sinne des § 3 Abs. 3 Niedersächsisches Datenschutzgesetz (NDSG) ist und damit die Verantwortung für die technisch und organisatorisch erforderlichen Maßnahmen nach § 7 NDSG trägt. Des Weiteren gehört zum Einsatz digitaler Medien an niedersächsischen Schulen nicht nur die Vermittlung der Handhabung von Programmen und Endgeräten, sondern ebenfalls die umfassende Vermittlung eines Datenschutzbewusstseins für Fragen des Grundrechtsschutzes, des Datenschutzrechtes, des Selbstdatenschutzes, der Informationssicherheit und anderer alltagsrelevanter rechtlicher Bereiche (wie beispielsweise Urheberrecht, Haftungsrecht im Netz, Computerstrafrecht, Onlineverträge, Telemedienrecht und Jugendmedienschutz).
Zudem braucht es entsprechend ausgewogene praktische Trainings, um das Gelernte in die gelebte Praxis umzusetzen. Hier wird deutlich, dass es nicht nur um einen neuen Baustein im Lehrplan geht, sondern um die frühzeitige engmaschige Verflechtung des so Gelernten und Trainierten im Gesamtcurriculum der Schullaufbahn. Das setzt voraus, dass die Lehrkräfte umfassend im Studium und durch Fortbildung für die vorgenannten Querschnittsthemen qualifiziert werden. Eine Aufgabenwahrnehmung durch neigungsorientierte Fachlehrer greift als Lösung zu kurz.

Weitere Informationen:

www.lfd.niedersachsen.de
> Themen > Schulen

Microsoft Office 365: Einsatz in Schulen unzulässig

Microsoft Office 365 ist ein Cloud-basiertes Büropaket, wobei Cloud Computing für Datenverarbeitung in der Wolke steht und eine über Netze angeschlossene Rechnerlandschaft beschreibt, in welche die eigene Datenverarbeitung ausgelagert wird. Die im Prinzip beliebig skalierbare Leistung kann dabei online variabel an die Bedürfnisse angepasst werden (so genanntes Provisioning). Auch Schulen interessieren sich dafür, weil das Konzept vor allem Kostenreduktion verspricht.

Will eine Schule von einem Cloud-Anbieter wie Microsoft IT-Dienstleistungen für Cloud-Services in Anspruch nehmen, so wird Letzterer als Auftragnehmer nach § 6 Niedersächsisches Datenschutzgesetz (NDSG) tätig. Die Schule bleibt für die Einhaltung sämtlicher datenschutzrechtlicher Bestimmungen verantwortlich. Sie hat einen Vertrag mit dem Cloud-Anbieter zu schließen.

Mindestanforderungen

Welche datenschutzrechtlichen Mindestanforderungen allgemein an das Cloud Computing zu stellen sind, wird im Artikel auf Seite 144 erläutert.[1] Dies gilt auch für Schulen. Insbesondere sind dies:

- Offene, transparente und detaillierte Informationen der Anbieter über die technischen, organisatorischen und rechtlichen Rahmenbedingungen der von ihnen angebotenen Dienstleistungen einschließlich der Sicherheitskonzeption, damit die Anwender klare Entscheidungskriterien bei der Wahl zwischen den Anbietern haben, aber auch, ob Cloud Computing überhaupt in Frage kommt.
- Transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Auftragsdatenverarbeitung, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität für den Fall, dass z. B. wegen einer Insolvenz des Anbieters die Datenverarbeitung zu einem anderen Anbieter „umziehen" muss.
- Umsetzung von abgestimmten Sicherheitsmaßnahmen auf Seiten von Cloud-Anbieter und Cloud-Anwender.
- Vorlage aktueller Zertifikate, welche die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird, zur Gewährleistung der Informationssicherheit und der beschriebenen Portabilität und Interoperabilität durch anerkannte und unabhängige Prüfungsorganisationen.

1 Siehe Beitrag „Datenschutzgerechtes Cloud Computing: Von der Kunst, Wolken transparent zu gestalten"

Keine Zusicherung für Datenverbleib in Europa

Da meiner Erfahrung nach Microsoft nicht bereit ist, sich im Rahmen der Auftragsdatenverarbeitung den Weisungen der Schule zu unterwerfen, ist der Einsatz von Office 365 nicht zulässig. Zudem konnte auf Nachfrage seitens des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Vertreter der Firma Microsoft nicht zweifelsfrei zugesichert werden, ob sich die Daten stets und ausnahmslos im europäischen Rechtsraum befinden und auch nicht zu entsprechenden Schichtzeiten (etwa im Supportfall) doch in ein außereuropäisches Land transferiert werden.

Was ist die Cloud?
Das Cloud Computing funktioniert nach dem Prinzip, dass abstrahierte IT-Infrastrukturen wie Kapazitäten für Rechenleistung, Speicher, Netzwerke oder auch fertige Software dynamisch an den Bedarf angepasst über ein Netzwerk zur Verfügung gestellt werden. Der Komfortvorteil wird darin gesehen, dass der Nutzer sich nicht um Infrastrukturen und technische Lösungen kümmern will und muss, sondern die zur Verfügung gestellte abstrahierte IT-Infrastruktur beliebig weit entfernt betrieben wird. Angebot, Beschaffung und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle sowie über lokale Browserfunktionen. Die Spannweite der Cloud-Leistungen umfasst unter anderem Infrastruktur (zum Beispiel Rechenleistung, Speicherplatz), Plattformen und Software.

Ausführliche Informationen in der Orientierungshilfe „Cloud Computing" der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, zu finden unter: www.lfd.niedersachsen.de > Technik und Organisation > Orientierungshilfen und Handlungsempfehlungen > Cloud Computing

4. Gesundheit und Soziales

Die elektronische Gesundheitskarte: Zahlreiche Fragen zum Foto

Ab Oktober 2011 begannen die gesetzlichen Krankenkassen, die ursprünglich bereits zum 1. Januar 2006 geplante Einführung der elektronischen Gesundheitskarte (eGK) schrittweise umzusetzen. Mit Ablauf des Jahres 2014 wurde die bisherige Krankenversicherungskarte dann endgültig durch die elektronische Karte ersetzt. Die neue eGK betraf rund 70 Millionen gesetzlich Versicherte in Deutschland und wurde zeitweise vor allem wegen des auf der Kartenvorderseite eingearbeiteten Lichtbilds des Versicherten kontrovers diskutiert. Mit Hilfe des Fotos soll der Versicherte leichter identifiziert und die missbräuchliche Inanspruchnahme von Leistungen verhindert werden können.

Zusätzlich zu den Versichertenstammdaten, die auch auf der alten Krankenversichertenkarte gespeichert wurden, soll es perspektivisch die Möglichkeit geben, freiwillige Zusatzfunktionen zu nutzen, wie zum Beispiel die Speicherung der Notfalldaten, elektronische Rezepte und auch Arztbriefe. Der verstärkte Einsatz von Telematikanwendungen verfolgt ebenfalls das Ziel, die Behandlungsprozesse im Gesundheitswesen zu optimieren und die Versorgungsqualität aller Beteiligten zu steigern. Auch die Kommunikationsprozesse sollen durch die eGK effektiver und transparenter gestaltet werden.

Aufgrund vieler offener datenschutzrechtlicher Fragen der letzten Jahre (Kartenlesegeräte, Notfalldatensatz, erweiterter Datensatz, NSA, Foto) hat sich der Blick auf die elektronische Gesundheitskarte geschärft. Insbesondere die Verpflichtung, ein Lichtbild zur Verfügung zu stellen, führte bei vielen Versicherten zu großem Unbehagen und zu zahlreichen Eingaben bei mir.

Mit Urteil vom 18. November 2014 (Az. B 1 KR 35/13 R) hat das Bundessozialgericht (BSG) meine Auffassung bestätigt, dass die Einführung der neuen Karte mit Lichtbild weder gegen bestehende datenschutzrechtliche Bestimmungen verstößt noch gegen das Recht auf informationelle Selbstbestimmung. Das Gericht wies damit die Revision eines Rentners aus Hessen zurück. Nach Ansicht des BSG ist die elektronische Gesundheitskarte in ihrer gegenwärtigen Ausgestaltung aufgrund überwiegender Allgemeininteressen gerechtfertigt. Diese Auffassung teile ich, daher wird die eGK in der aktuellen Form von mir nicht beanstandet.

Ausstattung von Pflegeheimen: Aufsicht und Sozialhilfeträger dürfen Daten austauschen

Im Berichtszeitraum habe ich mich mit der datenschutzrechtlichen Zulässigkeit der Kommunikation zwischen der Aufsichtsbehörde für Pflegeheime und dem Sozialhilfeträger befasst. Es gibt viele Gründe, warum beide Seiten miteinander Daten austauschen müssen, sei es im Rahmen von Pflegesatzvereinbarungen nach § 85 Sozialgesetzbuch – Elftes Buch (SGB XI), bei Personalprüfungen durch die Heimaufsicht zur persönlichen und fachlichen Eignung der Heimbetreiber oder deren Mitarbeiter oder bei Prüfungen der personellen Ausstattung der Heime.

Der Sozialhilfeträger ist nach § 85 Absatz 2 Nr. 2 SGB XI Vertragspartner der Pflegesatzvereinbarung. Bestandteile der Pflegesatzvereinbarung sind zum Beispiel wesentliche Leistungs- und Qualitätsmerkmale nach § 84 Absatz 5 SGB XI. Hier finden sich unter anderem Festlegungen zur personellen Ausstattung wie zum Beispiel

- die Festschreibung der zu erfüllenden Fachkraftquote,
- die Festlegung des Stellenanteils der verantwortlichen Pflegefachkraft und Pflegedienstleitung,
- die Benennung der verhandelten Personalschlüssel sowie
- die Anzahl der Auszubildenden.

Die dafür erforderlichen Daten erhält der Sozialhilfeträger wiederum von der für die Durchsetzung der Vorschriften des Heimgesetzes zuständigen Behörde (Heimaufsicht). Diese prüft regelmäßig die Bewohnerstruktur und personelle Ausstattung von Heimen mit dem Ziel, den Heimbewohnerinnen und Heimbewohnern eine bestmögliche und wirtschaftliche Pflege zukommen zu lassen, und übermittelt ihre Prüfungsergebnisse an den Sozialhilfeträger. Hierzu hat der Gesetzgeber die Aufforderung zu einer engen Zusammenarbeit zum Schutz der Bewohnerinnen und Bewohner in § 15 Abs. 1 Satz 1 Niedersächsisches Heimgesetz (NHeimG) geschaffen. Der Betreiber eines Pflegeheims bat mich, zu prüfen, ob die für ihn zuständige Heimaufsicht und der Sozialhilfeträger eventuell mehr Daten austauschen als erlaubt.

Spezieller Erlaubnistatbestand

Die Zulässigkeit der Datenübermittlung richtet sich nach dem speziellen Erlaubnistatbestand des § 15 Abs. 2 NHeimG. Hiernach ist die Heimaufsichtsbehörde berechtigt und verpflichtet, die für die Zusammenarbeit mit dem Träger der Sozialhilfe erforderlichen Angaben auszutauschen, einschließlich der bei den Prüfungen gewonnenen Erkenntnisse wie zum Beispiel bezüglich der personellen Ausstattung in Heimen. Gemäß Satz 2 sind personenbezogene Daten vor der Übermittlung grundsätzlich zu anonymisieren. Im Rahmen meiner Prüfung konnte ich feststellen, dass die gesetzlichen Vorgaben umgesetzt wurden, es gab daher keinen Anlass zu einer Beanstandung.
Der Petent hatte darüber hinaus moniert, dass die Aufgaben der Heimaufsicht und des Sozialhilfeträgers in derselben Organisationseinheit (Fachdienst) einer Behörde wahrgenommen würden. Hierzu teilte ich ihm mit, dass die Behördenorganisation dem kommunalen Selbstverwaltungsrecht (Organisationshoheit) unterfalle. Für die Beurteilung der Rechtmäßigkeit einer Datenübermittlung sei es unerheblich, welche organisatorische Zuordnung die Gebietskörperschaft getroffen habe.

Keine Regelungslücke

Das Niedersächsische Heimgesetz enthält entsprechende datenschutzrechtliche Regelungen zur Datenübermittlung zwischen diesen beiden Abteilungen. Aber auch wenn keine vorrangigen, spezialgesetzlichen Datenschutzvorschriften vorhanden sind, entsteht keine Regelungslücke. In diesen Fällen finden die Vorschriften des Niedersächsischen Datenschutzgesetzes (NDSG) Anwendung. Nach § 11 Abs. 4 NDSG sind die Vorschriften zur Übermittlung von Daten an andere öffentliche Stellen auf die Weitergabe von Daten innerhalb derselben öffentlichen Stelle, auch zwischen zwei eigenständigen Abteilungen innerhalb eines Fachdienstes derselben Behörde, entsprechend anwendbar. Die rechtlichen Voraussetzungen und Grenzen für die Übermittlung von Daten sind dieselben. Daher habe ich keinen Grund gesehen, diese Art der Organisation zu beanstanden.

Datenschutz und Kindesunterhalt: Eltern sind zur Auskunft verpflichtet

Geht es um Unterhaltszahlungen, wird gerne versucht, die eigenen finanziellen Verhältnisse vor dem anderen Elternteil oder dem Kind geheim zu halten. Als Argumentationshilfe dient häufig der Datenschutz, sodass auch ich immer wieder mit diesen Fällen befasst bin.

Leben die Eltern eines Kindes getrennt, kommen die Regeln des Familienunterhalts nicht mehr in Betracht. Beide Elternteile haben jedoch dafür Sorge zu tragen, dass dem Kind ein angemessener Unterhalt geleistet wird (§ 1610 Bürgerliches Gesetzbuch – BGB). Das Gesetz kennt allerdings keine festen Sätze, wie dieser angemessene Unterhalt auszufallen hat. 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. Der andere Elternteil hat seinen angemessenen Unterhalt in Form von Barunterhalt zu leisten. Die Unterhaltsbedarfssätze ergeben sich aus gerichtlichen Tabellen, in der Praxis werden häufig die Unterhaltssätze der so genannten Düsseldorfer Tabelle angewandt. Hierzu ist es erforderlich, die Höhe des monatlichen Einkommens des betreffenden Elternteils zu ermitteln.
Nach § 1605 BGB sind Verwandte in gerader Linie, also Eltern und Kinder, einander verpflichtet, auf Verlangen über ihre Einkünfte und ihr Vermögen Auskunft zu erteilen, soweit dies zur Feststellung eines Unterhaltsanspruchs oder einer Unterhaltsverpflichtung erforderlich ist. Über die Höhe der Einkünfte sind auf Verlangen Belege, insbesondere Bescheinigungen des Arbeitgebers, vorzulegen.

Jugendamt nimmt die Rechte des Kindes wahr

Sofern das Jugendamt als Beistand im Sinne des § 68 Sozialgesetzbuch – Achtes Buch (SGB VIII) tätig wird, ermittelt es den Unterhaltsbedarf für das Kind und prüft die Leistungsfähigkeit der zum Unterhalt Verpflichteten. Im Rahmen dieser Tätigkeit hat das Jugendamt die entsprechenden Nachweise zu erheben.
Die unterhaltspflichtigen Elternteile haben beide das Recht zu überprüfen, ob die Berechnung des zu leistenden Unterhalts korrekt erfolgt ist. Werden deshalb die vom Beistand notwendigerweise erhobenen Daten zu den Einkünften der Mutter an den ebenfalls unterhaltspflichtigen Vater des Kindes (und umgekehrt) weitergegeben, so ist dies nach § 68 SGB VIII datenschutzrechtlich nicht zu beanstanden.
Zum Wohle des Kindes hielte ich allerdings ein gemeinsames Gespräch beim Jugendamt für sinnvoller als eine Beschwerde bei der Datenschutzbeauftragten.

Krebsregistrierung in Niedersachsen: Meldepflicht und Datenschutz austariert

Mit der am 7. Dezember 2012 verabschiedeten Novellierung des Gesetzes über das Epidemiologische Krebsregister Niedersachsen (GEKN) wurde erstmals eine generelle Meldepflicht für Krebserkrankungen eingeführt. Hintergrund aus Sicht des Gesetzgebers: Je umfangreicher und vollständiger die Informationen über Krebserkrankungen sind, desto eher können die Krebs verursachenden Gründe ermittelt und gegebenenfalls verhindert werden. Zu berücksichtigen war, dass es sich bei den Daten im Krebsregister um sehr sensible Patientendaten handelt.

Der Datenschutz spielt nahezu bei jedem Paragrafen des GEKN eine wichtige Rolle. Bereits im Gesetzgebungsverfahren war Schwerpunkt meiner Arbeit, die Einführung einer Meldepflicht von personenbezogenen Daten zu einer Krebserkrankung mit dem Recht auf informationelle Selbstbestimmung des Patienten in Einklang zu bringen.

Neu: Widerspruchsrecht im GEKN

Mit der Einführung des Widerspruchsrechts in § 4 GEKN ist es gelungen, die Qualität und Quantität der Meldungen zu steigern und gleichzeitig die Datenschutzrechte der Patienten zu wahren. Der Patient erhält die Möglichkeit, der dauerhaften Speicherung seiner Identitätsdaten in der Vertrauensstelle, einer vom eigentlichen Krebsregister getrennten und beim Landesgesundheitsamt eingerichteten Treuhandstelle, nach erfolgter Meldung zu widersprechen. Die personenbezogenen Daten werden nur zur Bildung der Kontrollnummer verwendet, und die Registerstelle erhält in diesen Fällen nur noch einen faktisch anonymisierten Datensatz. Nach Weiterleitung der medizinischen Daten werden in der Vertrauensstelle alle Daten gelöscht, sodass ein Patientenbezug nicht mehr möglich ist.

Zahlreiche Rückfragen, wenige Probleme

Das novellierte GEKN trat am 10. Dezember 2012 in Kraft. Erwartungsgemäß führte das nahezu völlig neue Gesetz zu Beginn des Jahres 2013 sowohl bei den Ärzten als auch bei den Patienten zunächst zu vermehrten Rückfragen. Die vorbildliche Aufklärung und Arbeit des Epidemiologischen Krebsregisters hat sicherlich einen großen Anteil daran, dass bis zum heutigen Tage keine datenschutzrechtliche Beanstandung erforderlich war.

Landesgesetz zum KFRG noch komplexer

Aufgrund des am 3. April 2013 beschlossenen Krebsfrüherkennungs- und -registergesetzes (KFRG) ist nunmehr auch beabsichtigt, behandlungsbegleitende klinische Krebsregister zu schaffen. Ziel dieses Gesetzes ist es, eine Krebserkrankung möglichst frühzeitig zu erkennen, die Behandlung so erfolgreich wie möglich durchzuführen und die Qualität der onkologischen Behandlung insgesamt zu verbessern. Anstatt bundeseinheitliche Regelungen vorzugeben, wurden die Länder aufgefordert, flächendeckend klinische Krebsregister einzuführen, in welchen alle relevanten Behandlungsdaten zu einer Person gespeichert werden. Zur Umsetzung des KFRG ist auf Länderebene ein entsprechendes Gesetz notwendig.
Zu der ohnehin schon äußerst komplexen Materie, siehe GEKN, kommt hinzu, dass ein entsprechendes Landesgesetz auch die Fälle abdecken sollte, in denen ein Patient aus einem anderen Bundesland oder dem Ausland in Niedersachsen mit- oder weiterbehandelt wird oder ein Niedersachse sich in einem anderen Bundesland oder im Ausland behandeln lässt. Die klinischen Krebsregister sollen behandlungsbegleitend zur Verfügung stehen. Zum Wohle des Patienten müsste somit auch ein Zugriff eines ausländischen Arztes ermöglicht werden. Ob und wie dies datenschutzkonform in einem Landesgesetz umgesetzt werden kann, bleibt abzuwarten.
Zum Ende des Berichtszeitraums befand sich das „Gesetz über das klinische Krebsregister Niedersachsen – GKKN“ noch in der Entwurfsfassung. Ich werde das Gesetzgebungsverfahren datenschutzrechtlich begleiten.

Krankenhausinformationssysteme: Bundesweit einheitliche Orientierungshilfe weiter verbessert

Dass Krankenhäuser nicht mehr ohne Informationstechnik arbeiten können, ist wenig überraschend. Dass es sich bei den Patientendaten um hochsensible personenbezogene Daten handelt, ist ebenfalls jedem betroffenen Patienten, aber auch allen Beteiligten in den Medizin- und Pflegeberufen sowie den Krankenhausverwaltungen bewusst. Der Datenschutz in einem Krankenhaus muss deshalb einen besonders hohen Stellenwert haben. Dies fordern Patienten und Datenschützer gleichermaßen. Bei Prüfungen in verschiedenen Ländern sind teilweise beträchtliche Defizite in den Bereichen Datenschutz und ärztliche Schweigepflicht im Zusammenhang mit der Nutzung von Krankenhausinformationssystemen (KIS) festgestellt worden. Die tatsächliche Praxis der Datenverarbeitungsprozesse ist zudem in Jahrzehnten unterschiedlich gewachsen. Auch die eingesetzten Technologien und Fachverfahren sind heterogen.

Um die datenschutzkonforme Gestaltung und Nutzung von Informationstechnik in Krankenhäusern sicherzustellen, bedurfte es der Festlegung einheitlicher Anforderungen. Statt unterschiedlicher Bewertungen lautete aus Sicht der Datenschutzbehörden das Ziel, zu einem bundesweit und trägerübergreifend einheitlichen Verständnis zu kommen, was die gemeinsamen Beurteilungsgrundlagen rechtlicher Art und für technisch-organisatorische Maßnahmen zum Datenschutz anbelangt, bezogen auf Daten, Prozesse und Organisation sowie IT-Systeme und -Infrastruktur.

Einheitliche Anforderungen seit 2011

Bereits 2011 hatte hierzu eine Unterarbeitsgruppe der Arbeitskreise Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) unter Mitarbeit von Datenschutzbeauftragten der Evangelischen Kirche in Deutschland und des Datenschutzbeauftragten der Norddeutschen Bistümer der Katholischen Kirche eine „Orientierungshilfe Krankenhausinformationssysteme“ (OH KIS, Version 1) erarbeitet. Für die Datenschutzbehörden sollte dieses Dokument als Maßstab bei der künftigen Bewertung konkreter IT-Verfahren im Rahmen ihrer Kontroll- und Beratungstätigkeit dienen (siehe auch meinen XXI. Tätigkeitsbericht, Seite 13).
In der praktischen Anwendung heißt dies auch, einen ständigen Prozess der Qualitätsüberprüfung der Orientierungshilfe zu realisieren. Stellen die Datenschutzbehörden im Zuge ihrer Kontrolltätigkeit Defizite im Vergleich zu den dargelegten Maßstäben fest, so werden sie auf die Krankenhäuser einwirken und sie dabei unterstützen, in einem geordneten Prozess unter Wahrung der Patientensicherheit Wege zur Behebung der Defizite zu finden. Die Erfahrungen der Prüftätigkeit sollen

in eine regelmäßige Überarbeitung und Aktualisierung der Orientierungshilfe unter Berücksichtigung der technischen Weiterentwicklung einfließen. Die Arbeitskreise hatten von der DSK den Auftrag erhalten, diesen Revisionsprozess zu koordinieren. Die Deutsche Krankenhausgesellschaft e. V. (DKG)[1] als gemeinnütziger Interessen- und Dachverband von Spitzen- und Landesverbänden der Krankenhausträger und die jeweiligen Landeskrankenhausgesellschaften, so auch die Niedersächsische Krankenhausgesellschaft e. V.[2], wurden und werden dabei einbezogen.

15 Sitzungen, Szenarien, Workshops

Seit 2012 sammelte und bewertete die Unterarbeitsgruppe änderungsbedürftige Punkte. Durch Textänderungen entstand nach 15 Sitzungen am 18. Februar 2014 unter Federführung der Berliner Kollegen eine überarbeitete Fassung, die der AK Technik noch im selben Monat beschloss. Teil I (Rechtliche Rahmenbedingungen) wurde auch deshalb präzisiert, um Verständnisschwierigkeiten zu begegnen. Als Beispiel sei der Begriff der Sperrung genannt, der in verschiedenen Landeskrankenhausgesetzen definiert ist und eine andere Bedeutung als der gleichlautende Begriff im allgemeinen Datenschutzrecht hat. Die Orientierungshilfe wählt daher stattdessen den Begriff Zugriffsbeschränkungen. Außerdem befasste sich die Arbeitsgruppe mit einem Katalog von Szenarien des zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern.

Die Arbeitsgruppe konnte in gemeinsamen Workshops mit Vertretern der Deutschen Krankenhausgesellschaft einen intensiven Fachdialog führen sowie Übereinstimmung zu den in der Orientierungshilfe formulierten Anforderungen erzielen. Eingeflossen in die neue Fassung sind vor allem erste Prüferfahrungen der Datenschutzbeauftragten mit der Umsetzung der Orientierungshilfe in den Krankenhäusern, die Auswertung von Pilotprojekten, aber auch An-

1 Die Deutsche Krankenhausgesellschaft e.V. (DKG) ist ein gemeinnütziger Interessen- und Dachverband von Spitzen- und Landesverbänden der Krankenhausträger; http://www.dkgev.de/

2 Niedersächsische Krankenhausgesellschaft e.V.; http://www.nkgev.de/

regungen von Landeskrankenhausgesellschaften und kirchlichen Krankenhausdatenschutzbeauftragten. Die Deutsche Krankenhausgesellschaft veröffentlichte als empfehlenswerte Hilfestellung die „Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme".[3]

Neue Version seit März 2014 verfügbar

Die neue Version 2 der Orientierungshilfe wurde am 31. März 2014 fertiggestellt.[4] Sie ist wie folgt gegliedert:

- Vorwort,
- Begleitpapier,
- Glossar,
- Teil I „Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen",
- Teil II „Technische Anforderungen an die Gestaltung und den Betrieb von Krankenhausinformationssystemen (Teil I und Teil II wurden gegenüber der ersten Fassung beibehalten. Neben einigen inhaltlichen Änderungen wurden die Texte redaktionell mit dem Ziel einer besseren Lesbarkeit und Verständlichkeit überarbeitet. Teil II nimmt nun durchgängig Bezug auf die rechtlichen Anforderungen des Teils I),
- Katalog von „Szenarien zulässigen Datenaustauschs zwischen stationären und ambulanten Leistungserbringern".

Den Vergleich zwischen den beiden Versionen des Teils I erleichtert ein neues Papier „Rechtliche Rahmenbedingungen für den Einsatz von Krankenhausinformationssystemen – Synopse der Fassungen 2011 und 2014", das die Unterarbeitsgruppe Krankenhausinformationssysteme der Arbeitskreise Gesundheit und Soziales sowie Technische und organisatorische Datenschutzfragen der DSK zusätzlich erstellt hat.

3 Deutsche Krankenhausgesellschaft e.V. (DKG): Hinweise und Musterkonzepte für die Umsetzung der technischen Anforderungen der Orientierungshilfe Krankenhausinformationssysteme, 2. überarbeitete Fassung vom 25. März 2014, http://www.lfd.niedersachsen.de/download/86184/Information_der_DKG.pdf

4 Die Orientierungshilfe, 2. Fassung, vom 31. März 2014 und alle anderen Dokumente stehen auf meiner Themenseite „Orientierungshilfe Krankenhausinformationssysteme" bereit: www.lfd.niedersachsen.de > Navigation > Themen > Gesundheit > Krankenhaus; Deeplink: http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=13016&article_id=95681&_psmand=48; Deeplink zur Orientierungshilfe als PDF: http://www.lfd.niedersachsen.de/download/57482/Orientierungshilfe_Krankenhausinformationssysteme_Version_2.pdf

Datenschutz in medizinischen Forschungsprojekten: Intensive Beratungsgespräche mit der TMF

Die Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF)[1], ein gemeinnütziger Verein mit 91 Mitgliedern, stellt unter anderem Gutachten, Leitfäden und IT-Anwendungen sowie Schulungs- und Beratungsangebote bereit. Ziel des Vereins ist es, die organisatorischen, rechtlichen und technologischen Voraussetzungen für die klinische, epidemiologische und translationale Forschung zu verbessern. Förderer sind das Bundesministerium für Bildung und Forschung (BMBF), der Projektträger Gesundheitsforschung im Deutschen Zentrum für Luft- und Raumfahrt (DLR) sowie die Deutsche Forschungsgemeinschaft (DFG).

Die TMF hat Nutzungs- und Lizenzbedingungen entwickelt, die grundsätzlich die freie Verfügbarkeit der Ergebnisse für die medizinische Forschung garantieren. Gleichzeitig wird damit sichergestellt, dass Rückmeldungen von den Anwendern an die TMF zurückfließen und in der Weiterentwicklung der Produkte berücksichtigt werden können. Als Beispiel sind besonders die Werkzeuge zur Konzeption datenschutzgerechter Datensammlungen, die „Generischen Datenschutzkonzepte", oder als Werkzeug zur Pseudonymisierung der „PID-Generator" zu nennen. Eine Zusammenarbeit der Datenschutzbeauftragten mit diesem gemeinnützigen Verein verspricht unter Berücksichtigung dieser Rahmenbedingungen einen großen Mehrwert aus präventiver Sicht des Datenschutzes. Der Mehrwert wird verstärkt durch die Tatsache, dass eine bundesweit und sogar grenzüberschreitend flächendeckende und multiplikative Wirkung für Vorgaben in Form eines Leitfadens für generische und modifizierbare Musterlösungen für zahlreiche Forschungsprojekte erzielt wird.

1 Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), http://www.tmf-ev.de/

Leitfaden nach zehn Jahren erneuert

Medizinische Forschung arbeitet immer häufiger im vernetzten Zusammenwirken in Forschungsverbünden, nicht selten mit internationalen Dimensionen. Als maßgeblicher Aspekt für den Forschungserfolg gilt bei diesen Verbünden, dass die globale oder überregionale Zusammenführung und Bereitstellung aller für die Forschung relevanten Daten in zentral verfügbaren Datenbanken erfolgt. Nur so werden die für Forschung erforderlichen Synergieeffekte erzielt. Die Arbeitsgruppe Datenschutz der TMF hat bereits 2003 den Leitfaden zum Datenschutz in medizinischen Forschungsprojekten (Version 1) entwickelt. Auch damals wurde dieser Leitfaden mit den Arbeitskreisen Wissenschaft sowie Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) abgestimmt. Ziel war die Bereitstellung eines einheitlichen Bezugsrahmens und einer Blaupause für die Abstimmung konkreter Datenschutzkonzepte in der medizinischen Verbundforschung, zum Beispiel Kompetenznetze der Medizin, mit den zuständigen Datenschutzaufsichtsbehörden.

Verzahnung mit Datenschutzkonzept für Biobanken

In der Arbeitsgruppe Datenschutz der TMF wurden in der Folge dieser Abstimmprozesse in zehn Jahren bis 2013 über 50 Forschungsprojekte in Bezug auf eine datenschutzgerechte Umsetzung von Daten- und Probensammlungen beraten und 20 Forschungsprojekte dahingehend begutachtet. Diese später in der TMF-Schriftenreihe publizierten generischen Lösungen wurden 2006 um ein generisches Datenschutzkonzept für Biobanken ergänzt, das wiederum mit dem Arbeitskreis Wissenschaft der DSK abgestimmt worden war. Aufgrund einiger Veränderungen in den strukturellen, förderpolitischen und auch gesetzlichen Rahmenbedingungen war eine umfassende Überarbeitung der generischen Konzepte von 2003 und eine engere und konkret nachvollziehbare Verzahnung mit dem Konzept für Biobanken von 2006 nötig geworden.
Ein überarbeiteter Entwurf zur Version 2 des Leitfadens zum Datenschutz in medizinischen Forschungsprojekten vom 17. März 2013 wurde im Mai 2013 zur Abstimmung mit den Arbeitskreisen Wissenschaft sowie Technische und organisatorische Datenschutzfragen der DSK vorgelegt. Das Gesamtkonzept enthält nach Überarbeitung insgesamt vier Module, die je nach Zielrichtung des einzelnen Forschungsverbundes einzeln oder auch kombiniert verwendet werden können:

- Klinisches Modul (bisher Modell A),
- Studienmodul (neu, für klinische Studien, die den Vorschriften des Arzneimittelgesetzes oder des Medizinproduktegesetzes unterliegen),
- Forschungsmodul (bisher Modell B) sowie
- Biobankenmodul (bisher als separates Konzept vorhanden).

Workshop in Berlin

Am 29. August 2013 wurde ein Workshop mit acht TMF- und Forschungsvertretern unter Leitung von Univ.-Prof. Dr. Klaus Pommerening und insgesamt 15 Datenschutzvertretern durchgeführt. Aus meiner Behörde nahmen an dem Workshop die beiden für Datenschutz in der Forschung und für Gesundheitsdaten sowie für technisch-organisatorischen Datenschutz und Datenschutz in Telemedien zuständigen Referatsleiter teil. Die Agenda umfasste im Kern zentrale Aspekte der Aktualisierung des Leitfadens, insbesondere:

- Rechte- und Rollenaspekte/Verhinderung von Rollenkonflikten, Mandantentrennung (auf die Orientierungshilfe Mandantenfähigkeit der DSK wird nun im Leitfaden referenziert[2]),
- Abgrenzung von Versorgung und Forschung,
- organisatorische und rechtliche Umsetzung der informationellen Gewaltenteilung – Kriterien der Verhältnismäßigkeit und Lösungsansätze –,
- Relativität des Personenbezugs bei pseudonymen Daten,
- Broad Consent[3] – Anwendungsfälle, Lösungsansätze, Grenzen sowie
- technische Umsetzungsmöglichkeiten des Klinischen Moduls.

Alle geplanten Fragestellungen wurden in fachlichen Diskussionen des Workshops zu einer konsensfähigen Abstimmungsreife geführt. Viele Anregungen der Aufsichtsbehörden nahm die Arbeitsgruppe der TMF in die redaktionelle Aufarbeitung zur Anpassung, Korrektur und Präzisierung auf. Die TMF überarbeitete sodann den Entwurf für den neuen „Leitfaden zum Datenschutz in medizinischen Forschungsprojekten – Generische Lösungen der TMF – Version 2" und legte nach inhaltlichen Abstimmungs- und Kommentierungsrunden mit den Datenschutzbeauftragten die finale Fassung vom 5. März 2014 den Arbeitskreisen der DSK vor. Diese empfahl schließlich im März 2014 den medizinischen Forschungseinrichtungen und Forschungsverbänden, den Leitfaden als Basis zu nehmen für die konkrete Ausgestaltung ihrer Datenschutzkonzepte. Näheres findet sich auf der Website der TMF[4].

2 Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit – des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 1.0 vom 11. Oktober 2012, auf meiner Website www.lfd.niedersachsen.de unter > Technik und Organisation > Orientierungshilfen und Handlungsempfehlungen > Mandantenfähigkeit; Deeplink: http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=31646&article_id=109520&_psmand=48

3 Broad consent oder open consent ist eine Einwilligungsform zur Datenverarbeitung in der Forschung, die keine eng gefasste Einwilligung auf einen bestimmten Verwendungszweck beinhaltet (klassisches Modell), sondern die die Forschungsrichtung, in die mit dem Forschungsmaterial geforscht wird, breit und offen lässt. Damit wollen involvierte Forschungseinrichtungen den Zugang auf das Forschungsmaterial (etwa Biomaterial) erhalten, ohne vorher explizit genannt worden zu sein.

4 Website der TMF mit der neuen Fassung des Leitfadens http://www.tmf-ev.de/News/articleType/ArticleView/articleId/1518.aspx

5. Datenschutzbeauftragte in Behörden und

Behördliche Datenschutzbeauftragte: Kontaktdaten und eigene Mailadresse Mangelware

Nach § 8 a Abs. 3 S. 4 Niedersächsisches Datenschutzgesetz (NDSG) können sich alle Personen, die sich durch eine öffentliche Stelle in ihrem Recht auf informationelle Selbstbestimmung verletzt fühlen, mit ihrem Anliegen unmittelbar an die behördlichen Datenschutzbeauftragten (behDSB) wenden. Die behDSB nehmen daher in den öffentlichen Stellen eine datenschutzrechtliche Ombudsfunktion sowohl für die Belange der Beschäftigten als auch für die Bürgerinnen und Bürger wahr. Zur Gewährleistung der Vertraulichkeit haben die öffentlichen Stellen durch organisatorische Maßnahmen sicherzustellen, dass diese Eingaben den behDSB unmittelbar zugehen (§ 7 NDSG).

In dem Berichtszeitraum habe ich stichprobenartig die Internetpräsenz von rund 100 Kommunen, 250 Schulen und diversen Landesbehörden zum Thema Datenschutz und zur Außenwirkung der behördlichen Datenschutzbeauftragten überprüft. Es stellte sich heraus, dass die Homepages der öffentlichen Stellen nur wenige Informationen zum Thema Datenschutz und oftmals gar keine Kontaktdaten der oder des behDSB enthielten. Auf meine Hinweise und Empfehlungen richteten fast alle angeschriebenen Stellen dem behDSB umgehend eigene E-Mail-Adressen und abgeschottete Postfächer ein, außerdem wurden die Kontaktdaten des behDSB veröffentlicht und Vertretungsregelungen organisiert.

Sehr viele Schulen ohne Datenschutzbeauftragten

Bei der Überprüfung fiel auf, dass es zirka 80 Prozent der Schulleitungen nicht bewusst war, dass sie – in Abstimmung mit den Schulpersonalräten – einen Datenschutzbeauftragten zu bestellen haben. Sie gingen irrtümlich davon aus, dass die Landesschulbehörde Niedersachsen oder die jeweiligen Schulträger diese Aufgaben für die Schulen mit wahrzunehmen haben. Insbesondere im Schulbereich bedarf es aus meiner Sicht in den nächsten Jahren noch weitergehender Aufklärung zu datenschutzrechtlichen Belangen, aber auch verstärkter Kontrollen durch die Landesdatenschutzbeauftragte.
Ich appelliere an die Behörden- und Schulleitungen, die Arbeit der behDSB zu unterstützen und – sofern nötig – die bestehenden Arbeitsbedingungen zu verbessern. Eine wirksame Aufgabenwahrnehmung erfordert, die behördlichen Datenschutzbeauftragten, sofern sie die Aufgabe nicht bereits hauptamtlich ausüben, im jeweils erforderlichen Umfang von anderen Tätigkeiten zu entlasten. Im Hinblick auf den Aufgabenbestand der behördlichen Datenschutzbeauftragten reicht es nicht aus, diese Aufgabe einer oder einem Bediensteten zusätzlich zu seinen sonstigen Aufgaben „zur Erledigung nebenbei“ zu übertragen. Es bedarf der Freistellung im erforderlichen Umfang: Den behördlichen Datenschutzbeauftragten sind angemessene zeitliche Ressourcen zur Verfügung zu stellen, um ihre Aufgabe wirksam ausüben zu können.

Unternehmen

Netzwerkpflege: Wissenstransfer durch NORD–WEST und SÜD–OST

Die Kooperation mit den behördlichen Datenschutzbeauftragten der öffentlichen Stellen ist ein wichtiger Bestandteil meiner täglichen Arbeit. Ohne deren Unterstützung wäre die zeitnahe Umsetzung datenschutzrechtlicher Ziele vor Ort in einem Flächenland wie Niedersachsen nicht möglich.

Die halbjährlich stattfindenden Treffen der seit vielen Jahren etablierten Netzwerke NORD–WEST und SÜD–OST, an denen jeweils 20 bis 40 kommunale Datenschutzbeauftragte teilnehmen, sowie der jährliche Erfahrungsaustausch der behördlichen Datenschutzbeauftragten in meinem Hause sind inzwischen geschätzte Plattformen, um Wissen auszutauschen und sich zu datenschutzrechtlichen Themen fortzubilden. Die Mitglieder der Netzwerke arbeiten mit meiner Unterstützung gemeinsam engagiert und problemorientiert aktuelle Themen des Datenschutzalltags auf und tragen wirksam zur Stärkung und Verbesserung des Datenschutzes in der Region bei. Mein Dank richtet sich an die Ausrichter dieser Veranstaltungen.

Weitere Informationen: www.lfd.niedersachsen.de > Unser Netzwerk

Betriebliche Datenschutzbeauftragte: Viele Fragen zu Fachkunde und Interessenkonflikten

Für ein Unternehmen besteht gemäß § 4 f Abs. 1 Bundesdatenschutzgesetz (BDSG) die Pflicht zur Bestellung eines Datenschutzbeauftragten (DSB), wenn mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Viele Anfragen zu Aus- und Fortbildungsmöglichkeiten und der Unabhängigkeit spiegeln in meiner täglichen Praxis wider, dass immer noch in vielen Betrieben Unsicherheit herrscht, ob und wie die Bestellung eines betrieblichen Datenschutzbeauftragten umgesetzt werden soll.

Erschwerend kommt hinzu, dass eine spezifizierte Berufsanforderung rechtlich nicht festgelegt ist. In der gesetzlichen Vorgabe des § 4 f Abs. 2 BDSG werden die Anforderungen an den Datenschutzbeauftragten lediglich mit „Fachkunde“ und „Zuverlässigkeit“ beschrieben. Im Rahmen der Beratung zu Fragen der erforderlichen Fachkunde weise ich sowohl auf die bereits im Juni 2011 von der Mitgliederversammlung des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. publizierte Handreichung „Das berufliche Leitbild des Datenschutzbeauftragten“ hin, als auch auf die entsprechenden Bildungsangebote der verschiedenen etablierten Institutionen.

Abteilungsleiter sind ausgeschlossen

Auch werden von meiner Behörde immer häufiger Auskünfte zu möglichen Interessenkonflikten eingeholt, die geeignet sein könnten, die vom Gesetz geforderte Zuverlässigkeit der zu bestellenden Person in Frage zu stellen, insbesondere dann, wenn diese Person mit der Aufgabe des betrieblichen DSB nur „nebenamtlich“ betraut wird. Hierzu äußern sich Gola/Schomerus in ihrem Kommentar zum BDSG, 10. Auflage, in der Randbemerkung 5.6 wie folgt: „Die Bestimmungen über den Beauftragten für den Datenschutz bringen den Gedanken einer qualifizierten Selbstkontrolle zum Ausdruck. Daraus folgt, dass bestimmte Personen, unabhängig von ihrer Fachkunde und Zuverlässigkeit, nicht zum Datenschutzbeauftragten bestellt werden dürfen. Dies gilt ausnahmslos für den Inhaber selbst, den Vorstand, den Geschäftsführer oder den sonstigen gesetzlich oder verfassungsmäßig berufenen Leiter. Darüber hinaus sollen auch Personen nicht zum Datenschutzbeauftragten berufen werden, die in dieser Funktion in Interessenkonflikte geraten würden, die über das unvermeidliche Maß hinausgehen.“

In meiner behördlichen Praxis konzentrieren sich die Auskunftsersuchen vor diesem Hintergrund auf die Frage, ob die Inhaber bestimmter Arbeitsplätze, zum Beispiel die Leiterin oder der Leiter der IT-Abteilung bzw. der Personalabteilung, zugleich zum nebenamtlichen Datenschutzbeauftragten bestellt werden dürfen, weil sie oft durch ihr Wissen und ihre Expertise dem Unternehmen als besonders geeignet erscheinen. Gerade Personen, die in Unternehmen Leitungsfunktionen wahrnehmen, also Entscheidungskompetenzen aufweisen, kommen als Datenschutzbeauftragte nicht in Betracht und sind demzufolge von einer Bestellung auszuschließen.

Alternative: externer DSB

Aufgrund der mangelnden Auswahl unter den zur Verfügung stehenden geeigneten Mitarbeitern und der mit der Bestellung eines betrieblichen DSB verbundenen Kosten entscheiden sich heute viele kleinere Unternehmen vermehrt für ein Lösungskonzept mit einem entsprechend qualifizierten externen DSB. Allerdings zeigen die Anfragen auch, dass die Bedeutung des professionellen Umganges mit dem Datenschutz und auch die damit verbundene Stellung des qualifizierten und unabhängigen Datenschutzbeauftragten in den einzelnen Unternehmen zwar immer mehr in den Vordergrund rückt, aber längst noch keine Selbstverständlichkeit ist.

Brüssel will Voraussetzungen ändern

Nach dem Entwurf der EU-Datenschutz-Grundverordnung der EU-Kommission wird sich die Stellung des DSB im Unternehmen jedoch verändern. Der Entwurf beinhaltet, dass ein DSB nur dann bestellt werden muss, wenn das Unternehmen 250 oder mehr Mitarbeiter beschäftigt oder, unabhängig von der Mitarbeiterzahl, wenn seine Kerntätigkeit in der Durchführung von Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen. Der Begriff der Kerntätigkeit von Unternehmen ist dem deutschen Datenschutzrecht bisher fremd, und so wird sich vor allem die Frage stellen, was unter einer Kerntätigkeit zu verstehen ist. Man darf dabei wohl an die Tätigkeit von Auskunfteien, Marktforschungseinrichtungen und ähnlichen Unternehmen denken, deren direkter Geschäftszweck darin besteht, Daten von Personen zu erheben und diese Daten direkt wirtschaftlich zu verwerten. Von der präzisen Auslegung des unbestimmten Begriffs der Kerntätigkeit wird somit letztlich abhängen, ob kleine und mittlere Unternehmen auch tatsächlich zur Bestellung eines betrieblichen DSB verpflichtet sein werden oder ob die Bestellungspflicht letztlich nur die großen Unternehmen treffen wird.

Eine solche Entwicklung hätte gravierende Auswirkungen auf den Datenschutz insgesamt. In den Unternehmen sind es die betrieblichen Datenschutzbeauftragten, die dafür sorgen, dass personenbezogene Daten von Verbrauchern, Mitarbeitern und Kunden geschützt verarbeitet werden. Der betriebliche DSB kennt die Abläufe und Prozesse viel besser als Aufsichtsbehörden und ist die erste Anlaufstelle, um einen wirksamen Schutz von Kunden- und Mitarbeiterdaten durchzusetzen. Es bleibt deshalb zu hoffen, dass in den anstehenden Trilog-Verhandlungen eine Lösung gefunden wird, mit der der betriebliche DSB zweifelsfrei und umfassend verbindlich wird.

Weitere Informationen:

www.lfd.niedersachsen.de
> Themen > Datenschutzbeauftragte > Betriebliche Datenschutzbeauftragte

6. Datenschutz in der Wirtschaft

Datenschutz im Kraftfahrzeug: Gläserne Fahrer im rollenden Rechner

Die Autobranche ist im Umbruch: In wenigen Jahren wird das vernetzte Auto, das „connected car", Standard sein, es wird nicht nur über Internetverbindungen verfügen, sondern auch in der Lage sein, Verkehrszeichen zu erkennen und mit anderen Fahrzeugen, zum Beispiel zum Umfahren eines Staus, zu kommunizieren. Und autonom fahrende Kraftfahrzeuge (Kfz), die als Prototypen von verschiedenen Konzernen bereits vorgestellt wurden, sollen bis zum Jahr 2020 Marktreife erlangen. Die Zukunft hat schon begonnen.

Rund 130 Jahre nach Erfindung des Automobils, also des – seinem Namen nach – sich selbstständig bewegenden Mobils, fängt diese Erfindung an, ihren Namen mit Leben zu füllen: Die Kfz-Branche arbeitet seit Jahren an der Entwicklung des autonomen Kfz. Was hat diese Entwicklung mit Datenschutz zu tun? Sehr viel: Schon zum jetzigen Zeitpunkt werden in einem durchschnittlichen Kfz dutzende Datenkategorien erhoben und verarbeitet. Das Auto der Zukunft wird – in jeder seiner Entwicklungsstufen – massive Datenströme verarbeiten. Nicht nur die Datenmenge und die Übertragungsgeschwindigkeit, sondern auch die Anzahl an erhobenen personenbezogenen Daten wird enorm ansteigen. Hierbei muss man sich klarmachen, dass das vernetzte Kfz wie kaum ein anderes Produkt in der Lage sein wird, ein umfassendes Persönlichkeitsprofil zu erstellen:

- Tagesrhythmus,
- Bewegungsprofile,
- emotionale Komponenten (vorausschauender oder abrupter Fahrer?),
- Körpergröße (Sitzeinstellungen),
- Anzahl an Mitfahrern (Anzahl geschlossener Gurte),
- Telefonlisten,
- Musikgeschmack …

Aus der Zusammenlegung mehrerer Profile ließen sich unter anderem gemeinsame Treffen herauslesen.

Die Daten gehören dem Fahrer

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

Anders ist es bei personenbezogenen Daten, die im Zusammenhang mit dem Kfz anfallen. Daten sind dann personenbezogen, wenn sie sich auf eine bestimmte Person oder zumindest auf eine bestimmbare Person beziehen. Eine Person ist dann bestimmbar, wenn sie zum Beispiel über die Fahrgestellnummer oder weiteres Zusatzwissen identifizierbar ist. In diesen Fällen liegen also „personenbezogene Daten" vor. Damit gilt in diesen Fällen das Bundesdatenschutzgesetz (BDSG). Es enthält eine klare Aussage: Die Daten gehören dem Betroffenen. Auf das Kfz bezogen: Die Daten gehören dem Fahrer bzw. dem Halter des Kfz.

Zusammen mit meinen Datenschutzkolleginnen und -kollegen des Bundes und der Länder bin ich mir hierbei einig, dass auch technische Daten, die auf den ersten Blick weniger interessant erscheinen, aber personenbeziehbar sind, dem Bundesdatenschutzgesetz unterfallen. Beispielsweise erscheint die Anzahl der Bremsvorgänge auf den ersten Blick „weniger spannend". Auf einen konkreten Zeitraum bezogen gibt diese Information jedoch unter anderem Aufschluss darüber, ob der – identifizierbare – Fahrer zu einem „ruppigen" Fahrverhalten neigt oder vielleicht auch ein Stadtfahrer ist. Sofern diese Informationen ohne Zeitbezug gespeichert werden und regelmäßig wieder überschrieben werden, lassen sie sich zumindest durch ein enges Ausleseintervall einem konkreten Zeitraum zuordnen. Somit könnten bereits mit relativ wenigen Informationen einfache Persönlichkeitsprofile gebildet werden.

Forderungen der Datenschutzbeauftragten

Die Begehrlichkeiten für solche potentiellen Datensammlungen sind groß. Mögliche Interessenten sind Kreditkartenfirmen, Scoringunternehmen, potentielle Arbeitgeber und Versicherungen, wobei sich die Liste von möglichen Interessenten problemlos fortsetzen ließe. Das Bundesdatenschutzgesetz sorgt dafür, dass personenbezogene Fahrdaten nicht zu einem freien Wirtschaftsgut werden: Gemäß § 4 Abs. 1 BDSG dürfen diese Daten nur dann genutzt werden, wenn entweder eine gesetzliche Regelung dies erlaubt oder wenn der Betroffene (Fahrer/Halter) wirksam eingewilligt hat. Auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2014 habe ich mit meinen Kolleginnen und Kollegen eine Entschließung verabschiedet, die konkrete Forderungen an die Automobilindustrie richtet. Hierbei haben wir klargestellt, dass Datenverarbeitungen entweder vertraglich vereinbart sein müssen oder eine ausdrückliche Einwilligung vorliegen muss. Hierzu gehört zumindest vollständige und praxisnahe Transparenz. Aber auch bei einer vertraglich vereinbarten oder von einer Einwilligung getragenen Datenübertragung muss der Fahrer vom Hersteller in die Lage versetzt werden, eine solche Datenübermittlung zu erkennen, zu kontrollieren und gegebenenfalls zu unterbinden. Zudem muss Wahlfreiheit für datenschutzfreundliche Systemeinstellungen und die umfangreiche Möglichkeit zum Löschen eingeräumt werden.
Um konkrete Ergebnisse zu erzielen, führe ich seit Dezember 2014 gemeinsam mit einigen anderen Landesdatenschutzbeauftragten, die standortbedingt mit dem Thema befasst sind, sowie der Bundesdatenschutzbeauftragten Gespräche mit dem Verband der Automobilindustrie. Im nächsten Tätigkeitsbericht werde ich sicherlich von konkreten Ergebnissen berichten können.

Autos für Kunden, nicht für Labore

Was aber können die Autokäufer tun? Sie sind mächtiger, als sie glauben. Wichtig ist, dass die Kunden im jetzigen Entwicklungsstadium den Autoherstellern gegenüber artikulieren, dass sie – beim vernetzten Fahren oder wenn sie beim künftigen autonomen Auto gar das Lenkrad aus der Hand geben – die Kontrolle über ihre Fahrdaten behalten wollen. Autos werden nicht für Labore, sondern für Kundenwünsche hergestellt. Die Kunden müssen deutlich machen, dass sie eine Datenschleuder nicht akzeptieren, dass eine Datenschleuder also unverkäuflich sein wird. Nur dann werden, über die gesetzlichen Regelungen hinaus, praxisnahe datenschutzfreundliche Konzepte angeboten werden.

Weitere Informationen:

Entschließung der Datenschutzkonferenz vom 8./9. Oktober 2014 unter:
www.lfd.niedersachsen.de > DSB-Konferenzen > Entschließungen

Geldtransfer-Verordnung:
EU verlangt Daten bei Bareinzahlung

Ein Petent wollte wieder, wie früher, durch Bareinzahlung mit Zahlschein am Bankschalter seine Telefonrechnung begleichen. Als Grund gab er an, dass das weitverbreitete Online-Banking inzwischen zu indiskret geworden und die neu eingeführte verpflichtende Verwendung der SEPA-Formulare ein weiteres Indiz dafür sei, dass analoge Zahlweisen endgültig aufgegeben werden sollen.

Der Petent war der Ansicht, der Zahlungsverkehr solle in der EU offensichtlich möglichst lückenlos und automatisiert erfasst werden können. Dies wolle er aus Datenschutzgründen unbedingt vermeiden. Er begründete das mit seiner selbstständigen Tätigkeit in einem wirtschaftlich sehr diskreten Bereich und der dringenden Vermeidung von Rückschlüssen auf seinen Klientenstamm und seine Aufträge. Er fragte deshalb an, welche Daten bei Bareinzahlung mittels Zahlschein von ihm gegenüber dem Kreditinstitut offengelegt werden müssten und ob eine Ausweispflicht oder Übergabe einer Ausweiskopie gesetzlich gefordert sei.
Dem Petenten habe ich folgendes mitgeteilt:
Die EU-Verordnung 1781/2006 (Geldtransfer-Verordnung) verpflichtet alle deutschen Banken, bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung mitzuwirken. Diese Verordnung gilt unmittelbar als staatliches Recht auch für alle deutschen Banken und regelt die genaue Verfahrensweise. Sofern Geld bar eingezahlt wird, müssen Informationen zum Auftraggeber an die Bank des Begünstigten übermittelt werden. Folgende Daten des Einzahlenden werden dafür erfragt und erfasst:

- Name und Vorname,
- Geburtsdatum und Geburtsort.

Bei Beträgen über 1.000 Euro ist zusätzlich die Vorlage eines amtlichen Ausweises des Einzahlers erforderlich. Eine Kopie des Ausweises muss nicht gefertigt und vorgelegt werden.

Weitere Informationen: http://ec.europa.eu/finance/payments/transfers/index_de.htm

Rückabwicklung fehlgeleiteter Überweisungen: Adressenweitergabe nach Fristsetzung zulässig

Ein Finanzdienstleister unterrichtete seine Kundin darüber, dass der Arbeitgeber eines anderen Kunden versehentlich regelmäßig Beträge für vermögenswirksame Leistungen über einen Zeitraum von viereinhalb Jahren auf ihr Konto überwiesen habe.

Der Gesamtbetrag der ohne Rechtsgrund geleisteten Zahlungen betrug 1.700 Euro. Die Kundin wurde gebeten, diesen Betrag auf ihr Konto einzuzahlen und das Einverständnis zu erteilen, um diese Summe von ihrem Konto auf das Konto des anderen Kunden umbuchen zu können. Mit diesem Regulierungsvorschlag war die Kundin nicht einverstanden, da sich bei weiterer Prüfung herausstellte, dass ihr eigener Arbeitgeber seiner Verpflichtung ihr gegenüber nicht nachgekommen war, und ihr somit diese Zahlungen fehlten. Weiterhin machte sie geltend, dass sie ihre Kontoauszüge regelmäßig geprüft habe und von einer ordnungsgemäßen Zahlung durch ihren Arbeitgeber ausgegangen sei. Zudem sei es unverständlich, dass ein Kontoinhaber über viereinhalb Jahre fehlende Zahlungen nicht wahrgenommen habe.
Bei der Prüfung der Übermittlung der Anschrift der Kundin an den Kunden kam der Finanzdienstleister im Rahmen der nach § 28 Abs. 2 Nr. 2a Bundesdatenschutzgesetz (BDSG) durchzuführenden Interessenabwägung zu dem Ergebnis, dass der Kunde möglicherweise einen zivilrechtlichen Anspruch auf Herausgabe des fehlenden Betrages nach § 812 BGB habe. Das Unternehmen drohte der Kundin zweimal unter Fristsetzung an, bei Nichtzahlung ihre Anschrift dem Kunden mitzuteilen. Dem zwischenzeitlich eingeschalteten Anwalt teilte es mit, dass nach erfolglosem Ablauf einer Zahlungsfrist die Adresse seiner Mandantin dem Kunden übermittelt werde. Nach Ablauf der Frist erfolgte durch den Finanzdienstleister die Mitteilung an den Kunden. Daraufhin beschwerte sich der Anwalt bei mir über das Vorgehen.

Abkommen regelt Verfahren

Im „Abkommen der Spitzenverbände der Deutschen Kreditwirtschaft im Überweisungsverkehr“ vom 4. April 2011 ist geregelt, wie in den Fällen einer fehlgeleiteten Überweisung zu verfahren ist. Es besteht Einigkeit bei den Datenschutzaufsichtsbehörden, dass eine Rückabwicklung fehlgeleiteter Zahlungen nicht durch eine Berufung auf das Bankgeheimnis oder das Datenschutzrecht erschwert oder vereitelt werden darf. Die Aufsichtsbehörden betonen jedoch, dass der ungerechtfertigt Bereicherte in jedem Fall die Möglichkeit haben muss, die Überweisung rückabzuwickeln, bevor seine Daten an den Zahler übermittelt werden. Auch über den Datenumfang muss er zuvor unterrichtet werden.
Das Vorgehen des Finanzdienstleisters war somit datenschutzrechtlich nicht zu beanstanden.

Geldwäsche:
Hausverwaltung muss Bank Daten liefern

Eine Hausverwaltung, die für mehrere Eigentümer Wohnungen verwaltete, hatte auf den Namen einer Wohnungseigentümergemeinschaft (WEG) ein Bankkonto eröffnet. Die Hausverwaltung fühlte sich durch Mitarbeiter einer Bank unter Druck gesetzt, weil sie trotz entgegenstehender Vorschriften nach dem Wohnungseigentumsgesetz und Beschlüssen der Eigentümer weitreichende Datenbestände dieser Personen nach dem Geldwäschegesetz (GWG) dem Kreditinstitut übermitteln sollte. Andernfalls würden die Konten der Hausverwaltung gekündigt.

Zur regelmäßigen Aktualisierung der Kontounterlagen nach § 3 GWG und für die Kontrollrechte der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) forderte die Bank folgende Daten von der Hausverwaltung an:

- Liste der Eigentümer mit Nachweis der jeweiligen Wohnungsgrößen (zum Beispiel Kopie der Teilungserklärung),
- Verwaltervollmacht,
- Protokoll der letzten Eigentümerversammlung.

Das Erfordernis des Nachweises hinsichtlich der Größe der jeweiligen Wohnungen begründete das Geldinstitut mit der Verpflichtung, einen beherrschenden Einfluss in der Wohnungseigentümergemeinschaft feststellen zu müssen. Gegebenenfalls seien diese Eigentümer als „wirtschaftlich Berechtigte“ nach dem GWG zu erfassen und zu identifizieren.
Nach den Regelungen des GWG und den Ausführungen der BaFin ergibt sich für die Eröffnung und Aktualisierung eines WEG-Kontos folgende Rechtslage: Da die WEG nach § 10 Abs. 6 des Wohnungseigentumsgesetzes (teil-)rechtsfähig ist, hält die BaFin die Kontoführung auf den Namen der WEG für zuläs-

sig. Wird das Konto auf den Namen der WEG eröffnet, muss sich diese durch die Vorlage eines Protokolls der Miteigentümerversammlung legitimieren. Dies gilt auch für den verfügungsberechtigten Verwalter. Seine Vertretungsvollmacht ergibt sich aus dem Protokoll, in dem die Bestellung dokumentiert ist. Nach dem GWG hat das Kreditinstitut zu klären, ob die Kontoinhaberin (WEG) für einen wirtschaftlich Berechtigten handelt. In diesem Fall muss dieser nach Maßgabe des § 4 Abs. 5 GWG identifiziert werden. Die WEG muss als Kontoinhaberin erklären, dass sie die Geschäftsbeziehung nicht auf Veranlassung eines Dritten (also im Interesse eines Dritten), insbesondere nicht als Treuhänder, eingeht. Weiterhin kann anstelle der konkreten Ermittlung der Eigentumsanteile, die 25 Prozent übersteigen, auch eine Eigentümerliste vom Verwalter übersandt werden. Dabei ist der Verwalter in der Regel zu verpflichten, Veränderungen der Liste der Bank unaufgefordert anzuzeigen. Wird so verfahren, muss kein wirtschaftlich Berechtigter der WEG festgestellt werden. Dieses Absehen von der konkreten Ermittlung der Eigentumsanteile und verringerte Prüfpflichten sind nur aufgrund des geringen Risikos bei Wohnungseigentümergemeinschaften zulässig.

Vorlage von Kopien der Teilungserklärung nicht erforderlich

Die Hausverwaltung und das Kreditinstitut wurden von mir über die Rechtslage informiert. Danach sind Eigentümerlisten, Verwaltervollmacht und entsprechende Protokolle der WEG dem Kreditinstitut vorzulegen. Ich habe darauf hingewiesen, dass die Vorlage von Kopien der Teilungserklärungen generell nicht erforderlich ist. Zudem unterliegen die Daten dem bankinternen Datenschutz. Sie dürfen daher nicht zu anderen bankeigenen Zwecken verwendet werden und dienen allein den Kontrollrechten der BaFin.

Vervielfältigung von Personalausweisen: Einscannen und Speichern unzulässig

Im XXI. Tätigkeitsbericht 2011–2012 (Seite 42 f.) habe ich dargestellt, dass die von zahlreichen Unternehmen geübte Praxis des Vervielfältigens von Personalausweisen in vielen Fällen nicht zulässig ist. Erstmalig hat nun mit dem Verwaltungsgericht Hannover ein Gericht eine Entscheidung über die Vervielfältigungsproblematik getroffen und das Verfahren eines Logistikdienstleisters, der sich gegen meine Anordnung auf dem Klagewege zur Wehr gesetzt hatte, beendet.

Dieses in der Automobilbranche tätige Unternehmen hatte auf seinem Betriebsgelände mehrere tausend Kraftfahrzeuge abgestellt, die täglich – zumeist von Fahrern von Speditionen – abgeholt werden. Um den Speditionsvorgang zu überwachen, wurden die Personalausweise der Abholer eingescannt und auf einem eigenen Rechner gespeichert. Unter Androhung eines Zwangsgeldes hatte ich dem Unternehmen aufgegeben, das Einscannen von Personalausweisen zu unterlassen und die rechtswidrig gespeicherten Daten zu löschen.

Schwerwiegender Verstoß

Die gegen meine Anordnung erhobene Klage des Unternehmens hatte keinen Erfolg. Das Verwaltungsgericht bestätigte die Rechtmäßigkeit meiner aufsichtsbehördlichen Anordnung, es hielt diese Praxis ebenfalls für rechtswidrig. Nach Auffassung des Gerichts stellt das von dem klagenden Unternehmen praktizierte Verfahren des Scannens und Speicherns von Personalausweisen einen schwerwiegenden Verstoß gegen datenschutzrechtliche Vorschriften im Sinne des § 38 Abs. 5 Satz 2 Bundesdatenschutzgesetz dar. Entscheidend für die Beurteilung des Verfahrens seien die im Personalausweisgesetz (PAuswG) getroffenen Regelungen über

VG Hannover, Urteil v. 28. Novemver 2013 – Az: 10 A 5342/11

den Umgang mit personenbezogenen Daten. Nach der maßgeblichen Vorschrift des § 20 PAuswG sei der Personalausweis ein Identifizierungsmittel, das der Inhaber vorlege und vorzeige, um sich auszuweisen. Nach § 20 Abs. 2 PAuswG dürfe der Personalausweis weder zum automatisierten Abruf noch zur automatisierten Speicherung personenbezogener Daten verwendet werden. Das Gericht verweist darauf, dass hiernach insbesondere das Einscannen und Speichern des Personalausweises gesetzlich verboten ist. Nach Ansicht des Gerichts kommt es auch nicht darauf an, ob der Ausweisinhaber in die Maßnahme eingewilligt hat. Das Personalausweisgesetz als hier einschlägige Spezialvorschrift sehe eine rechtfertigende Einwilligung des Betroffenen nicht vor. Ob im Gegensatz zum Scannen auch das Kopieren unzulässig ist, wurde ausdrücklich offengelassen. Dazu erwähnte das Gericht am Rande, dass jedenfalls bei einer möglichen Identifizierung unter Anwesenden die Erstellung einer Kopie grundsätzlich nicht zulässig sein dürfte. Dies entspricht auch meiner Rechtsauffassung.

Weitreichende Folgen

Die Entscheidung stieß nicht nur in der Fachpresse, sondern auch in der Öffentlichkeit auf breites Interesse. Für die Unternehmenspraxis hat sie weitreichende Änderungen zur Folge. Viele Unternehmen scannen – oft aus Unwissenheit oder aus Bequemlichkeit – die Ausweise ihrer Kunden, Lieferanten oder sonstigen Personen, anstatt, nach Identifikation der Betreffenden durch Ausweisvorlage, die benötigten Daten herauszuschreiben. Ausreichend für die Identifikation des Geschäftspartners sind in der Regel die relevanten Grunddaten wie Vorname, Nachname und Adresse. Den immensen Überschuss an weiteren Daten wie Personalausweisnummer, Foto oder auch Unterschrift benötigen sie nicht.
In diesem Zusammenhang ist deutlich auf die Gefahr hinzuweisen, die solche privaten Personalausweisdatensammlungen bergen: Sie können zu den jährlich abertausenden Fällen von Identitätsdiebstählen, zum Beispiel nach Einbruch oder Hacking, führen, denen zumeist in einem weiteren Schritt betrügerische Aktivitäten (Bestellungen oder Zahlungsvorgänge) folgen. Wenn sich Unternehmen diesen Hintergrund bewusst machen, fällt es sicherlich leichter, den Sinn und Zweck des gesetzlichen Verbotes zu verstehen.

Schwerpunktprüfung Zeitarbeitsfirmen: Keine Verstöße festgestellt

In den letzten zwei bis drei Jahren erreichten mich zahlreiche Petitionen, die den Umgang von Arbeitsvermittlungsagenturen und Zeitarbeitsfirmen mit Beschäftigtendaten zum Inhalt hatten. Das Spektrum der bekanntgewordenen Fälle reichte von Bewerbungsunterlagen im Altpapiercontainer bis hin zu Fragen des technisch-organisatorischen Datenschutzes bei Online-Bewerbungen. Diese technisch-organisatorischen Fragen gaben mir Anlass, die Branche der Zeitarbeitsfirmen zum Gegenstand einer Schwerpunktprüfung zu machen.

Prüfungsgegenstand war eine Auswahl von fünf Zeitarbeitsfirmen, die ihren Sitz in Niedersachsen haben. In inhaltlicher Hinsicht wurde auf den technisch-organisatorischen Datenschutz beim Umgang mit Online-Bewerbungen abgestellt. Konkret ging es beispielsweise um die Art der Datenerhebung, den Inhalt der Einwilligung, den jeweiligen Zweck der Speicherung dieser Daten, die möglichen Empfänger bei Weitergabe der Daten sowie die Frage der Löschung in Zusammenhang mit der jeweiligen Zweckbindung. Es wurden keine Verstöße festgestellt.

Datenschutz an der Leine: Haustierversicherung muss alte Rechnungen zurückschicken

Als ein kleiner Grundkurs in Sachen Datenschutzdogmatik erwies sich der Fall einer Petentin, die sich bei mir über ihre Versicherung beschwerte, genauer gesagt: über die Haustierversicherung, die den Hund der Petentin gesundheitlich absicherte, sich jedoch weigerte, die eingereichten Rechnungen zurückzuschicken.

Der Hund, so die Petentin, habe nach Abschluss der Versicherung eine kostenintensive Behandlung erhalten müssen; hierfür habe die Versicherung auch gezahlt. Anschließend habe sie die seltene Krankengeschichte ihres Vierbeiners in einer Zeitschrift für Hundefreunde veröffentlichen wollen. Damit sollten auch andere Hundehalter informiert werden, um für ihre eigenen Vierbeiner in ähnlichen Fällen gewappnet zu sein. Hierfür bat die Petentin die Versicherung, ihr die alten Tierarztrechnungen mit den Details zur Krankengeschichte, die sie selbst bei der Versicherung eingereicht hatte, zurückzuschicken. Nun kommt überraschend der Datenschutz ins Spiel: Die Versicherung weigerte sich, die Rechnungen an die Petentin herauszugeben und begründete dies mit Datenschutz. Natürlich ging es nicht um den Datenschutz zugunsten des Hundes, sondern um personenbezogene Daten der Petentin auf den Rechnungen.
Wie ist die Rechtslage? Damit überhaupt Datenschutzbedenken bestehen, bedarf es – unabhängig vom spezifischen Sachverhalt – in der Regel dreier Beteiligter:

- Zunächst der Betroffene, auf den sich die Daten beziehen (untechnisch gesagt: „Dem die Daten gehören“).
- Sodann die verantwortliche Stelle, also demjenigen, der die Daten rechtmäßig zu einem bestimmten Zweck „hat“ und damit „etwas anfangen“ möchte.
- Und hier kommt nun der „Dritte“ ins Spiel: In der Regel möchte die „verantwortliche Stelle“ die Daten des Betroffenen einem Dritten zugänglich machen (seltener: die verantwortliche Stelle möchte die Daten – ohne einen Dritten – selbst zu einem anderen Zweck verwenden als vom Betroffenen oder vom Gesetz gestattet).

Versicherung beruft sich zu Unrecht auf Datenschutz

Auf den konkreten Fall bezogen: Betroffene war hier die Petentin, da es um Rechnungen ging, in denen ihre personenbezogenen Daten enthalten waren. Verantwortliche Stelle war die Versicherung: sie besaß die Papierrechnungen und berief sich auf Datenschutz. Es fehlt jedoch an einem Dritten, denn eine Weitergabe an einen Dritten war nicht beabsichtigt. Eine Herausgabe von Daten an den Betroffenen selbst (quasi: eine Rückgabe der Daten) ist grundsätzlich zulässig! Es bestehen also grundsätzlich keine datenschutzrechtlichen Gründe, dem Betroffenen eine Herausgabe der Daten an ihn selbst zu verweigern. Auch eine Verwendung zu anderen Zwecken als ursprünglich vorgesehen, und zwar gegen den Willen der Petentin, stand erkennbar nicht im Raum.
Die Versicherung berief sich daher zu Unrecht auf den Datenschutz. Dies konnte ich der Petentin mitteilen, so dass einer Veröffentlichung der Hundeleidensgeschichte nichts mehr im Wege stand. Manchmal freut man sich auch über unerwartetes Lob. In diesem Fall über die Freude der Petentin, die am Rande erwähnte, dass mit dieser positiven Antwort vielen Tieren viel Leid erspart bleibe.

Dreifachpanne: Versicherung verschickt Unterlagen Dritter

Wenn der Fehlerteufel einmal zuschlägt, dann bleibt es meist nicht bei einem Fehler. Dies kann auch im Versicherungsbereich passieren.

Ein Petent trug folgenden Sachverhalt an mich heran: Er hatte bei einem großen Versicherungskonzern Angebotsunterlagen angefordert. Per E-Mail erhielt der Petent daraufhin ein Angebot, das allerdings auf eine ihm fremde Frau zugeschnitten war und deren persönliche Daten enthielt. Der Petent meldete die Datenschutzpanne der Versicherung und bat erneut um ein Angebot. Das erhielt er in einer weiteren E-Mail, allerdings betraf es diesmal einen fremden Herrn. Dieses Angebot enthielt also wiederum personenbezogene Daten eines ihm Fremden. Nachdem der Petent auch die neuerliche Panne gemeldet hatte, entschuldigte sich die Versicherung für die beiden Fehler. Anschließend erhielt der Petent ein postalisches Schreiben der Versicherung. Dieses enthielt jedoch neben dem „richtigen" Angebot an den Petenten wiederum ein fremdes Angebot für einen weiteren unbekannten Herrn.

Jetzt wandte sich der Petent an meine Behörde. In dem von mir eingeleiteten Kontrollverfahren führte die Versicherung an, dass der erste und dritte Fall auf menschlichem Versagen beruhten; im zweiten Fall habe es sich um eine Softwarepanne gehandelt. In einem anschließenden Ordnungswidrigkeitsverfahren habe ich gegen die Versicherung wegen Aufsichtspflichtverletzung ein Bußgeld in Höhe von 5.000 Euro verhängt (siehe auch Seite 84).

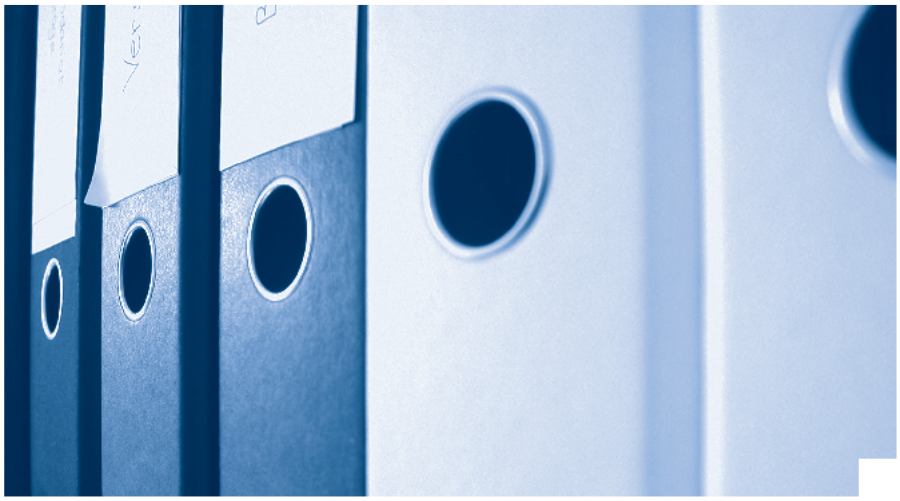
Unbefugte Weitergabe von Kundendaten: Wenn zwei sich streiten, freut sich der Dritte nicht immer

Einen Datenschutzfall der besonderen Art, der letztlich vier Aktenordner füllte, hatte ich im Bereich der lokalen Energieversorger zu bearbeiten. Im Kern ging es um die rechtswidrige Weitergabe von Kundendaten von einer Firma an eine andere und um 115 Beschwerden.

Lokale Energieversorger bieten großen Strom- und Gaskonzernen die Stirn; sie werben mit attraktiven Energiepreisen und mit dem Image des „David gegen Goliath". Niedrige Preise und lokales Image führen jedoch nur dann zu Wettbewerbsfähigkeit, wenn sie nicht auf Laienhaftigkeit und Unprofessionalität beruhen. Energieversorger A hatte mehrere tausend Kunden, aber sah sich ab einem bestimmten Zeitpunkt außerstande, diese selbst zu beliefern. Die Firma suchte daher einen Kooperationspartner, also einen anderen Energieversorger. Hierfür schloss der Vorstand von Firma A einen Kooperationsvertrag mit Firma B, ebenfalls ein lokaler Anbieter. Hiernach sollte Firma B die Strom- und Gasversorgung für die Kunden der Firma A übernehmen. Allerdings war der Kooperationsvertrag widersprüchlich bezüglich der Frage, ob es sich um eine rein interne Zulieferung handeln sollte und nach außen weiterhin Firma A auftreten dürfte, oder ob nach außen allein Firma B auftreten sollte.

Datenlieferung bereits vor Vertragsabschluss

An dieser Stelle ergibt sich ein erster Bezug zum Datenschutz: Der Kooperationsvertrag sah vor, dass Firma A die für die Belieferung nötigen Kundendaten an Firma B übergibt. Bei Firma B „tauchten" diese Daten auch „auf", allerdings schon vor Abschluss des Kooperationsvertrages. Es handelte sich unter anderem um die Adress- und Bankdaten der Kunden. Der genaue Weg, den die Kundendaten genommen hatten, ließ sich nicht ermitteln. In der Folge erhielten zahlreiche Kunden der Firma A Schreiben der Firma B, in denen sich Firma B als neuer Ansprechpartner vorstellte. Dies wiederum passte Firma A nicht. Sie schrieb daraufhin ihre Kunden an und teilte Folgendes mit:
„Wir möchten Sie in Kenntnis setzen, dass Kundendaten der Firma A, nach unserer Auffassung unrechtmäßig, durch die Firma B erlangt worden sind. Wir möchten Sie dringend bitten, Ihre Kontobewegungen laufend zu prüfen und verdächtigen Abbuchungen zu widersprechen. Eventuell sollten Sie anwaltliche Hilfe in Anspruch nehmen. (…) Falls Sie mit der Übermittlung Ihrer Daten an die Firma B nicht einverstanden sind und auch einer Datenübermittlung nicht ausdrücklich zugestimmt haben, sollten Sie den Landesbeauftragten für den Datenschutz Niedersachsen informieren. Dies kann per Brief oder Email geschehen. Wir haben für sie einen Mustertext bereitgestellt."



1.000 Euro Bußgeld festgesetzt

Auf diese Weise gingen bei meiner Behörde 115 Petitionen ein, die sich gegen eine unzulässige Datenverwendung durch Firma B wandten. Ich nahm die Petitionen zum Anlass, ein Datenschutzkontrollverfahren einzuleiten, und zwar gegen die Firma A aufgrund unbefugter Übermittlung personenbezogener Daten.
Zweifellos waren die Daten in Zusammenhang mit dem geplanten Kooperationsvertrag von Firma A an Firma B übergegeben worden. Die Unbefugtheit stand im Raum, weil der Kooperationsvertrag nicht ansatzweise erkennen ließ, welche Partei welche Pflichten trifft, also ob es sich zum Beispiel um eine Auftragsdatenverarbeitung handeln sollte. In diesem Fall wären etliche zusätzliche Detailregelungen im Vertrag erforderlich gewesen. Dass die Kundendaten schon vor Abschluss des Kooperationsvertrages bei Firma B vorlagen, kam erschwerend hinzu. Und es sei nur am Rande erwähnt, dass ich mich angesichts der offensichtlichen vertragsrechtlichen „Querelen" zwischen beiden Firmen durch die Bereitstellung des Mustertextes an die Kunden durch Firma A auch „vor den Karren gespannt" sah und die „Ahnungslosigkeit" der Firma A angesichts der schriftlich ausdrücklich vereinbarten Datenübermittlung nicht nachvollziehbar war.
Die rechtliche Prüfung ergab Folgendes: Einen Straftatbestand, also eine strafbare Datenübermittlung mit Bereicherungsabsicht, konnte ich ausschließen. Wegen der unbefugten Datenweitergabe war eine Datenschutzverletzung jedoch zu bejahen, so dass der Vorgang in einem Ordnungswidrigkeitsverfahren mündete. Als Ergebnis wurde ein Bußgeld in Höhe von 1.000 Euro festgesetzt.

E-Mail an alle, statt E-Mail für Dich: Datenschutzgerecht nur mittels bcc-Sendeoption

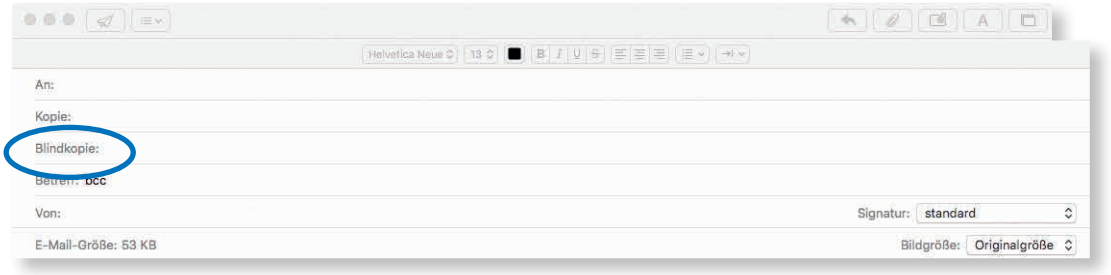
In der romantischen US-Filmkomödie führt der E-Mail-Austausch mit einem vermeintlich Unbekannten im Internet zum Happy End. In der Realität kann dies bereits im Vorfeld daran scheitern, dass eine E-Mail (versehentlich) gleich an alle versandt wird. Gerade rührige Vereinsmitglieder neigen dazu, Neuigkeiten und Informationen „in einem Rutsch" gleich allen kundzutun.

Jedoch stellt auch eine E-Mail-Adresse, die sich aus Namenbestandteilen zusammensetzt, grundsätzlich ein personenbezogenes Datum dar. Die Angabe der E-Mail-Adresse im Adressfeld „an" oder „cc" bewirkt somit datenschutzrechtlich zugleich eine Übermittlung dieses personenbezogenen Datums an alle anderen Adressaten der E-Mail. Eine solche Datenübermittlung ist jedoch nur zulässig, wenn entweder eine Einwilligung vorliegt oder eine gesetzliche Norm dieses Vorgehen rechtfertigt (§ 4 Abs.1 BDSG).
Eine ausdrückliche Einwilligung zur Übermittlung der eigenen E-Mail-Adresse an weitere Personen dürfte aber nur in den wenigen Fällen in Betracht kommen, in denen der Personenkreis, an den übermittelt wird, sehr überschaubar ist. Zu denken wäre hier zum Beispiel an die Mitglieder eines kleinen Vereins. Auch kann durch die Bereitschaft, E-Mails vom Verein zu empfangen, nicht gleichzeitig auf die Zustimmung zur Übermittlung der eigenen E-Mail-Adresse an eine Vielzahl Dritter geschlossen werden. Hierzu zählen auch die weiteren Vereinsmitglieder.
Eine Rechtsgrundlage ergibt sich auch nicht aus den klassischen Erlaubnistatbeständen des § 28 Abs. 1 S. 1 Nr. 1 oder Nr. 2 BDSG, insbesondere nicht bei Beachtung der Zweckbindung der Daten und dem Gebot der Datensparsamkeit. Die beliebige Übermittlung der E-Mail-Adresse an Dritte ist nämlich weder zur Begründung, Durchführung oder Beendigung der Vereinsmitgliedschaft, noch zur Wahrung berechtigter Interessen des Vereins, die das schutzwürdige Interesse des betroffenen Mitglieds überwiegen, erforderlich. Somit sind keine zwingenden Gründe ersichtlich, die das offene Versenden solcher E-Mail-Verteiler notwendig erscheinen lassen. Folglich ist die offene Übermittlung der E-Mail-Adresse im Adressfeld „an" oder „cc" unzulässig und stellt eine Ordnungswidrigkeit gemäß § 43 Abs. 2 Nr. 1 BDSG dar, die mit einer Geldbuße bis zu 300.000 Euro geahndet werden kann.

Es sind keine zwingenden Gründe ersichtlich, die das offene Versenden solcher E-Mail-Verteiler notwendig erscheinen lassen.

Verstöße mehrfach mit Bußgeld geahndet

Im Berichtszeitraum habe ich eine solche datenschutzwidrige E-Mail-Versendung bereits mehrfach mit einer Geldbuße geahndet. Dies lässt sich jedoch einfach vermeiden, wenn der Absendende bei der Versendung von E-Mails darauf achtet, dass alle E-Mail-Adressen in das Adressfeld „bcc" (Abkürzung für Blind Carbon Copy) eingetragen werden. Das Adressfeld „An" kann dabei auch leer bleiben. Dies bewirkt, dass die E-Mail als Kopie an alle eingegebenen Empfänger gesendet wird, der



Name und die E-Mail-Adresse jedoch für alle anderen Empfänger der Nachricht nicht sichtbar sind. Wer die E-Mail erhält, kann also nicht die weiteren Adressaten erkennen und erhält somit nicht unzulässig Daten übermittelt. Die Anonymität der einzelnen Empfänger bleibt gewahrt. Der bcc-Modus kann und sollte auch dann genutzt werden, wenn bei der Vereinskommunikation mit E-Mail-Verteilern oder Newslettern gearbeitet wird.

Auch beim Inhalt der E-Mail ist der Datenschutz zu beachten. Sofern die E-Mail einen weiteren Personenbezug enthält, kommt nur eine personenbezogene Versendung im Einzelfall in Betracht. So darf zum Beispiel eine E-Mail zur Erinnerung zahlungssäumiger Vereinsmitglieder nur an das betreffende Mitglied gesandt werden. Das bedeutet, dass der Kassenwart an jedes betroffene Mitglied eine eigene E-Mail senden muss, ohne „cc" oder „bcc" an weitere Vereinsmitglieder. Und selbst der Vorstand darf auf diesem Weg nicht ergänzend und wegen der Nutzung der „bcc"-Funktion für das kontaktierte Vereinsmitglied quasi heimlich mit informiert werden. Beim Weiterleiten von E-Mails, z. B. mit Informationen des Vorstands, ist darauf zu achten, dass die sich dann im Inhaltsfeld der Nachricht befindlichen vorherigen E-Mail-Adressen vor dem Weiterleiten gelöscht werden.

Bei sensiblen Informationen E-Mails verschlüsseln

Vereine sollten also einerseits selbst aufmerksam mit dem personenbezogenen Datum der E-Mail-Adresse umgehen und andererseits die Mitarbeitenden, aber auch Trainer und Betreuer entsprechend schulen, um unzulässige Datenübermittlungen zu vermeiden. Diese sollten im Umgang mit den oben beschriebenen Verwendungsmöglichkeiten von E-Mails informiert werden und dazu angehalten werden, im Zweifel immer auf die „bcc"-Sendeoption zurückzugreifen.

Ohnehin sollte bei der Vereinskorrespondenz per E-Mail immer hinterfragt werden, ob eine E-Mail für personenbezogene Daten überhaupt das angemessene Kommunikationsmedium ist. Bei sensiblen Informationen wie etwa einer Zahlungserinnerung sollte auf jeden Fall zumindest die Möglichkeit einer verschlüsselten E-Mail-Übermittlung genutzt oder eine Versendung auf dem Postweg erwogen werden. Darüber hinaus sollte, bei einer Erhebung und Speicherung von E-Mail-Adressen der Mitglieder im Rahmen einer wirksamen, informierten Einwilligung nach § 4 a BDSG, auf die Freiwilligkeit, den Zweck der Speicherung und die Verwendung (z. B. zur Zusendung von Informationen zu Punktspielen oder anderen Vereinsaktivitäten) hingewiesen werden.

Sofern Mitglieder den E-Mail Austausch mit anderen wünschen, können sie selbstverständlich die eigene E-Mail-Adresse bekannt geben. Der Verein sollte hier jedoch nicht vorgreifen.

Weitere Informationen: www.lfd.niedersachsen.de > Themen > Vereine > Orientierungshilfe Datenschutz im Verein

Führungszeugnisse ehrenamtlicher Übungsleiter:

Nach den Skandalen der vergangenen Jahre sollen sich die Träger der öffentlichen Jugendhilfe gemäß § 72 a Abs. 1 S. 2 Sozialgesetzbuch, Achtes Buch (SGB VIII) zur effektiven Durchsetzung des in Satz 1 geregelten Beschäftigungs- und Vermittlungsverbots ein Führungszeugnis nach § 30 Abs. 5 und § 30 a Abs. 1 des Bundeszentralregistergesetzes (BZRG) vorlegen lassen. Diese Regelung hat bei (Sport-)Vereinen in der Vergangenheit zunehmend zu einem Beratungsbedarf geführt. Es ist davon auszugehen, dass dies zukünftig auch Gegenstand von Eingaben sein wird.

§ 72 a SGB VIII verfolgt das Ziel, einschlägig vorbestrafte Personen von der Wahrnehmung von Aufgaben in der Kinder- und Jugendhilfe fernzuhalten und auszuschließen und damit Kindeswohlgefährdungen vorzubeugen. Anliegen des Gesetzgebers ist es, das erweiterte Führungszeugnis als Element eines umfassenden Präventions- und Schutzkonzeptes zur Verbesserung des Schutzes von Kindern zu etablieren. Ziel ist es, dass auch im Bereich des ehrenamtlichen und bürgerschaftlichen Engagements Minderjährige besser geschützt werden. Daher sollen nach § 72 a Abs. 2 und 3 SGB VIII die Träger der öffentlichen Jugendhilfe durch Vereinbarungen mit den Trägern der freien Jugendhilfe sicherstellen, dass diese keine Personen beschäftigen, die dem Schutzzweck des § 72 a nicht entsprechen. Die freien Träger können folglich ebenfalls die Vorlage eines Führungszeugnisses verlangen. Aus dem Wortlaut des § 72 a Abs. 3 und 4 SGB VIII wird deutlich, dass sich die Tätigkeit in einem pädagogischen Kontext abspielen muss („beaufsichtigt", „betreut", „erzieht", ausbildet"). Daher beschränkt sich § 72 a SGB VIII auf die reine Kinder- und Jugendarbeit. Sofern eine ehrenamtliche Person also wie eine hauptberufliche Person tätig wird, ist daher die Schwelle für ein Führungszeugnis erreicht. Wer hingegen nur punktuell oder vereinzelt in solchen pädagogisch sensiblen Bereichen tätig ist, dürfte in der Regel nicht zur Vorlage eines Führungszeugnisses verpflichtet sein.

Nicht alle Daten sind für die Eignungsfeststellung erforderlich

Für einen (Sport-)Verein, der die Aufgabe eines Trägers der öffentlichen Jugendhilfe wahrnimmt, bedeutet dies, dass diesem von seinen ehrenamtlichen Übungsleitern das Führungszeugnis vorzulegen ist. Da der Verein nach außen hin durch seinen Vorstand vertreten wird (§ 26 Abs. 1 BGB), ist auch diesem das Führungszeugnis vorzulegen. Das Führungszeugnis ist nach § 30 Abs. 1 BZRG von der betreffenden Person zu beantragen. Es wird aber unmittelbar dem Träger der öffentlichen Jugendhilfe übersandt. Problematisch kann es dabei sein, dass in einem Führungszeugnis alle eintragungsfähigen Vorkommnisse enthalten sind, während die Vorschrift selbst nur auf bestimmte Straftaten abstellt, so dass dem Empfänger des Führungszeugnisses Kenntnisse verschafft werden, die für die Eignungsfeststellung unerheblich sein könnten und somit nicht erforderlich sind.
Das Führungszeugnis wird nur zur Einsicht vorgelegt (§ 72 a Abs. 5 SGB VIII). Dabei dürfen die in der öffentlichen Jugendhilfe tätigen Vereine nach § 72 a Abs. 5 S. 1 SGB VIII von den eingesehenen Daten nur erheben,

- den Umstand, dass Einsicht in ein Führungszeugnis genommen wurde,
- das Datum des Führungszeugnisses und
- die Information, ob die das Führungszeugnis betreffende Person wegen einer Straftat nach Absatz 1 Satz 1 rechtskräftig verurteilt worden ist. Hierzu zählt beispielsweise der sexuelle Missbrauch von Schutzbefohlenen (§ 174 StGB).

Was darf der Verein erfahren und speichern?

Erlaubt ist nur die Erhebung, also das Beschaffen von Daten über die betroffene Person zu den zuvor genannten Sachverhalten, die nach § 72 a Abs. 1 SGB VIII relevant sind und ein Beschäftigungs- und Vermittlungsverbot rechtfertigen. Dies bedeutet, dass die darüber hinaus im Rahmen der Vorlage des erweiterten Führungszeugnisses eingesehenen Daten (zum Beispiel Straßenverkehrsdelikt) des Ehrenamtlichen aufgrund der oben erwähnten enumerativen Beschränkung nicht im datenschutzrechtlichen Sinne erhoben werden dürfen.
Eine Erlaubnis zur Speicherung enthält § 72 a Abs. 5 S. 1 SGB VIII hingegen ausdrücklich nicht. Nur im Satz 2 findet sich eine Ausnahme für die Speicherung. Hiernach darf der Träger der öffentlichen Jugendhilfe die erhobenen Daten nur speichern, verändern und nutzen, soweit dies zum Ausschluss der Personen von der Tätigkeit, die Anlass zu der Einsichtnahme in das Führungszeugnis gewesen ist, erforderlich ist. Es dürfen nur die drei oben genannten zulässig erhobenen Daten gespeichert werden, und dies auch nur, wenn der Betroffene aufgrund der Vorstrafen von der neben- oder ehrenamtlichen Tätigkeit ausgeschlossen werden muss oder soll. Enthält das Führungszeugnis keine Eintragungen und soll der Ehrenamtliche daher tätig werden, wäre eine Speicherung der erhobenen Daten unzulässig.

Eventuell neutralen Treuhänder einschalten

Auf den Fall des in der Jugendhilfe tätigen Vereins bezogen, bedeutet dies, dass dieser zum Beispiel gegenüber der Kommune als Träger der öffentlichen Jugendhilfe lediglich verbindlich erklären würde, dass er in das Führungszeugnis Einsicht genommen hat. In begründeten Zweifelsfällen oder bei Differenzen im Verein wäre gegebenenfalls die Einschaltung eines neutralen Treuhänders denkbar, der Einsicht in das Führungszeugnis nimmt und anschließend gegenüber dem Träger der öffentlichen Jugendhilfe die nach § 72 a Abs. 5 S. 1 SGB VIII zulässig einsehbaren Daten bestätigt.
Nach § 72 a Abs. 5 S. 3 und 4 SGB VIII zulässig gespeicherte Daten sind vor dem Zugriff Unbefugter zu schützen und unverzüglich zu löschen, wenn im Anschluss an die Einsichtnahme keine Tätigkeit aufgenommen wird. Andernfalls sind die Daten gemäß Satz 5 spätestens drei Monate nach der Beendigung einer solchen Tätigkeit zu löschen. Diese Regelung ist jedoch missverständlich, denn schließlich können Daten nur gelöscht werden, wenn sie zuvor gespeichert wurden. Eine Speicherung bei jugendhilferechtlich unbedenklicher Aufnahme einer Tätigkeit wäre nach den vorherigen Vorschriften jedoch unzulässig.

Einwilligung in Speicherung ist möglich

Allerdings ist die Speicherung von Daten unabhängig hiervon zulässig, wenn der Betroffene in die Speicherung eingewilligt hat. Die Einwilligung ist eine widerrufliche, freiwillige und eindeutige Willenserklärung der betroffenen Person, einer bestimmten Datenverarbeitung, etwa der Speicherung, zuzustimmen. Sie muss schriftlich erfolgen, und die betroffene Person muss über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufgeklärt werden. Außerdem muss sie unter Darlegung der Rechtsfolgen darauf hingewiesen werden, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft auch wieder widerrufen kann.

Schuldnerdaten: Keine Werbung durch Nutzung des Internetportals www.insolvenzbekanntmachungen.de

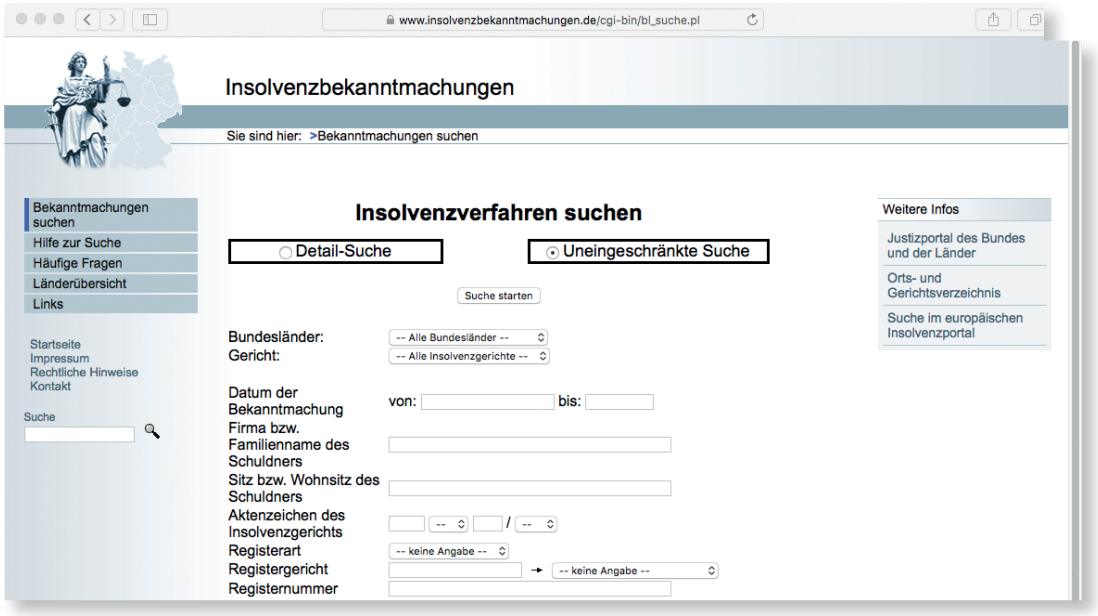
Im Berichtszeitraum lagen mir zahlreiche Beschwerden Betroffener vor, die von einem Unternehmen deshalb Werbung per Briefpost erhalten hatten, weil ihnen kurz nach erfolgreich abgeschlossenem Insolvenzverfahren die Restschuldbefreiung nach Maßgabe des § 300 Insolvenzordnung (InsO) erteilt worden war. Gegenstand der Werbung war dabei das Angebot des Unternehmens, für den Ex-Schuldner Auskunftsersuchen nach § 34 Bundesdatenschutzgesetz (BDSG) an Unternehmen zu richten, die Informationen zu seinem Insolvenzverfahren haben konnten, und mit Blick auf die erteilte Restschuldbefreiung anschließend die Löschung eventuell noch gespeicherter Informationen zu erwirken.

Die für die werbliche Ansprache notwendigen Informationen hatte das Unternehmen dem Internetportal www.insolvenzbekanntmachungen.de entnommen. Dort sind die Insolvenzbekanntmachungen von allen deutschen Insolvenzgerichten einschließlich der dazu erforderlichen personenbezogenen Daten der Schuldner für zwei Wochen öffentlich zugänglich. Vor diesem Hintergrund war der datenschutzrechtlichen Frage nachzugehen, ob die in amtlichen Bekanntmachungen insbesondere aus Gründen des Gläubigerschutzes offenbarten personenbezogenen Schuldnerdaten daneben auch für werbliche Zwecke genutzt werden dürfen, ohne dass die Betroffenen ihre Einwilligung dazu erteilt haben.
Entscheidend für die Beurteilung dieser Frage war, ob das Internetportal www.insolvenzbekanntmachungen.de als allgemein zugängliches Verzeichnis im Sinne von § 28 Abs. 3 Satz 2 Nr. 1, 2. Alt. BDSG anzusehen ist. Denn nur aufgrund dieser Vorschrift hätte die in Rede stehende Werbung datenschutzgerecht erfolgen können. Als Regelbeispiele für allgemein zugängliche Verzeichnisse nennt der Gesetzgeber in § 28 Abs. 3 Satz 2 Nr. 1, 2. Alt. BDSG Adress-, Rufnummern- oder Branchenverzeichnisse. Die in solchen Verzeichnissen enthaltenen personenbezogenen Daten haben den Zweck, es jedermann bei Bedarf (aus persönlichen und/oder geschäftlichen Gründen) zu ermöglichen, mit der verzeichneten Person/Firma in Kontakt treten zu können. Deshalb gelangen diese Daten regelmäßig mit Einwilligung bzw. auf Betreiben des Betroffenen in derartige Verzeichnisse.

Insolvenz-Portal darf nicht für Werbung „angezapft“ werden

Hingegen dient die Internetseite www.insolvenzbekanntmachungen.de ausschließlich als zentrale und länderübergreifende Plattform, auf der die öffentlichen Bekanntmachungen der Insolvenzgerichte zu erfolgen haben (§ 9 Abs. 1, Satz 1 InsO); sie verfolgt die folgenden Zwecke:

1. Gläubigerschutz: Durch die öffentliche Bekanntmachung wird sichergestellt, dass tatsächliche und/oder potenzielle Gläubiger von den in einem Insolvenzverfahren relevanten Tatsachen (z. B. Ankündigung einer Restschuldbefreiung) Kenntnis erhalten und somit vor dem möglichen Ausfall ihrer Forderung in der Insolvenz eines Schuldners bewahrt werden.
2. Verfahrensgerechte Zustellung: Die öffentliche Bekanntmachung genügt zum Nachweis an alle in einem Insolvenzverfahren Beteiligte (§ 9 Abs. 3 InsO).



Ferner ist eine uneingeschränkte Suche „Alle Insolvenzgerichte" für jedermann nur für Veröffentlichungen aus den letzten zwei Wochen möglich (§ 2 Abs. 1 Nr. 3 InsoBekV). Danach ist nur noch eine Detailsuche möglich, bei der der Sitz des Insolvenzgerichtes und mindestens eine der unter § 2 Abs. 1 Nr. 3 InsoBekV genannten Angaben erfolgen muss. Der Zugriff auf Schuldnerdaten kommt über das Portal nach Ablauf der zwei Wochen also nur mit Zusatzwissen in Betracht. Auch diese eingeschränkte Zugriffsmöglichkeit zeigt, dass sich das Insolvenzbekanntmachungen-Portal nicht an die allgemein interessierte Öffentlichkeit richtet, um diese jederzeit und nach Belieben zu informieren bzw. dieser personenbezogen Daten zur Kenntnis zu geben, damit ein persönlicher und/oder geschäftlicher Kontakt hergestellt werden kann.

§ 9 Abs. 1 der Insolvenzordnung (InsO) in Verbindung mit § 2 der Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet (InsoBekV) vom 12. Februar 2002 (BGBl. I S. 677) bestimmt, dass die öffentlichen Bekanntmachungen durch eine zentrale und länderübergreifende Veröffentlichung im Internet erfolgen.

Aus den vorgenannten Gründen ist die Internetseite www.insolvenzbekanntmachungen.de nicht mit Adress-, Rufnummern- oder Branchenverzeichnissen vergleichbar und kann somit auch nicht als allgemein zugängliches Verzeichnis im Sinne von § 28 Abs. 3 Satz 2 Nr. 1, 2. Alt. BDSG gelten. Diese Internetseite stellt vielmehr eine allgemein zugängliche Quelle im Sinne von §§ 28 Abs. 1 Satz 1 Nr. 3, 29 Abs.1 Nr. 2 BDSG dar, die jedoch wegen der spezialgesetzlichen Regelungen zur Werbung im § 28 Abs.3 BDSG nicht für werbliche Zwecke „angezapft" werden darf. Bereits aus diesen Überlegungen folgt, dass die oben beschriebene werbliche Ansprache datenschutzwidrig war.

Schutzwürdiges Interesse ehemaliger Schuldner überwiegt

Gleichwohl bin ich im Rahmen meiner Prüfung hilfsweise der Argumentation des für seine Dienste werbenden Unternehmens gefolgt, das die Internetseite www.insolvenzbekanntmachungen.de doch als allgemein zugängliches Verzeichnis betrachten wollte. Somit wäre die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung gemäß § 28 Abs. 3 Satz 2 Nr. 1, 2. Alt. BDSG zulässig gewesen, soweit schutzwürdige Interessen des Betroffenen (z. B. eines ehemaligen Schuldners) nicht entgegengestanden (§ 28 Abs. 3 Satz 6 BDSG) hätten.

Die Verletzung schutzwürdiger Interessen ergibt sich regelmäßig aus der Art der betroffenen Daten, kann aber auch im Verwendungszusammenhang bestehen bzw. sich aus der Gruppenzugehörigkeit ergeben[1]. Dies ist zum Beispiel der Fall, wenn durch die Art und Weise der Zusammenstellung der

1 Bergmann/Möhrle/Herb, BDSG § 28, Rn. 408

Daten mehr Informationen offen gelegt werden als die in § 28 Abs. 3 Satz 2 BDSG aufgezählten normalerweise vermitteln[2]. Zu diesen Daten, den so genannten Listendaten, gehören

- Gruppenzugehörigkeit,
- Beruf-, Branchen- oder Geschäftsbezeichnung,
- Name,
- Titel und akademische Grade,
- Anschrift und
- Geburtsjahr.

Unter der Internetadresse www.insolvenzbekanntmachungen.de werden hingegen nicht nur Listendaten, sondern auch weitere für ein Insolvenzverfahren relevante Daten veröffentlicht wie zum Beispiel eine rechtskräftige Ankündigung der Restschuldbefreiung, der Beginn der Wohlverhaltensperiode sowie gegebenenfalls Name und Anschrift einer Betreuerin oder eines Betreuers. Anhand dieser weiteren Daten sind Rückschlüsse auf die persönliche Lebenssituation des Betroffenen möglich, die über den Informationsgehalt der Listendaten deutlich hinausgehen. Ferner handelt es sich zusätzlich um Informationen, die den Lebensabschnitt eines Schuldners betreffen, der für diesen ohnehin unter erschwerten Bedingungen zu bewältigen ist. Zu nennen sind hier unter anderem die erheblich eingeschränkte Verfügungsgewalt über finanzielle Mittel, die eingeschränkte Teilhabe am gesellschaftlichen Leben, ein vermindertes Selbstwertgefühl sowie eine verminderte gesellschaftliche Anerkennung.
Somit waren eine Verarbeitung oder die Nutzung der aus dem genannten Internetportal erhobenen personenbezogenen Daten für Zwecke der Werbung gemäß § 28 Abs. 3 Satz 2 Nr. 1, 2. Alt. BDSG auch deshalb unzulässig, weil hier schutzwürdige Interessen der Betroffenen entgegenstehen (§ 28 Abs. 3 Satz 6 BDSG).

Unzulässige Zweckänderung

Außerdem scheiterte die datenschutzrechtliche Zulässigkeit des beschriebenen Geschäftsmodells auch daran, dass die über die Quelle www.insolvenzbekanntmachungen.de erhobenen Daten grundsätzlich nur zweckgebunden verarbeitet und genutzt werden dürfen (§ 16 Abs. 4 BDSG). Dieser datenschutzrechtliche Grundsatz der Zweckbindung sollte durch die Werbeaktion aber in rechtswidriger Weise gerade umgangen werden, so dass auch eine datenschutzrechtlich unzulässige Zweckänderung vorlag.
Vor diesem Hintergrund konnte das Geschäftsmodell datenschutzrechtlich nicht hingenommen werden. In mehreren Gesprächen mit Vertretern des Unternehmens und seiner Rechtsbeistände, in denen ich auch auf die Ordnungswidrigkeit der bis dahin betriebenen zahlreichen werblichen Ansprachen und auf die nach § 43 Abs. 3 Satz 2 BDSG bestehende Möglichkeit der Gewinnabschöpfung hinwies, gelang es mir schließlich, das Unternehmen zum Verzicht auf die Erhebung von Schuldnerdaten aus dem Portal und zu einer Änderung seiner Werbestrategie zu bewegen.

2 Simitis, BDSG § 28, Rn 245

Selbstauskünfte von Mietinteressenten: Für Besichtigungstermin reichen die Kontaktdaten

In Zeiten knappen Wohnraums, der vor allem in Großstädten zu beobachten ist und zu einer Verschiebung des Wohnungsmarktes zugunsten der Vermieter führt, scheuen diese zunehmend nicht davor zurück, sich die Lebensverhältnisse der Mietinteressenten bis ins Detail darlegen zu lassen und auch ungewöhnliche Fragen zu stellen. Eine Frage nach der Familienplanung mag da fast noch zurückhaltend erscheinen.

Eine von den Datenschutzaufsichtsbehörden erarbeitete Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressenten gibt Mietern und Vermietern Antwort darauf, welche Fragen ein Vermieter im Rahmen eines Vermietprozesses wann zulässig stellen darf. Der Vermieter muss zunächst ein berechtigtes Interesse an der Beantwortung der Fragen haben, die erfragten Daten müssen daher im Kontext mit dem angestrebten Mietverhältnis stehen und erforderlich sein, um eine Entscheidung über den Abschluss eines Mietvertrages mit einem konkreten Bewerber treffen zu können. Dabei sind die Interessen des Vermieters gegen das Recht auf informationelle Selbstbestimmung des Mietinteressenten abzuwägen.
Der Umfang des Fragerechts hängt davon ab, in welcher Phase sich der Vermietprozess befindet: Geht es zunächst nur um einen Besichtigungstermin, dürfen Vermieter oder die von ihnen beauftragten Makler nur solche Daten von Mietinteressenten erheben und verarbeiten, die für die Durchführung der Besichtigung wichtig sind, vor allem also Name und Kontaktdaten. Sofern der Mietinteressent erklärt, die Wohnung anmieten zu wollen, sind weitere Fragen zulässig. Welche das jeweils sind, ergibt sich aus § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG). Danach ist das Erheben personenbezogener Daten oder ihre Nutzung als Mittel für eigene Geschäftszwecke nur zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen Schuldverhältnisses, also eines Vertrages mit dem Betroffenen, erforderlich ist. Die Darlegung der Einkommensverhältnisse des Interessenten zur Klärung seiner Bonität darf der Vermieter daher erst einfordern, wenn er sich für einen Mieter entschieden hat. Gleiches gilt für die Einholung von Bonitätsauskünften bei Wirtschaftsauskunfteien.

Persönliche Daten erst bei Miet- oder Kaufabsicht

Dieser Verfahrensweise steht auch nicht der bisweilen von Immobilienmaklern vorgebrachte Hinweis auf eine Verpflichtung zur Identifizierung (mit Name, Geburtsort, Geburtsdatum, Staatsangehörigkeit und Anschrift) nach dem Geldwäschegesetz entgegen. Das Bundesministerium der Finanzen hat nämlich bereits mit Schreiben vom 7. Dezember 2012 an den Immobilienverband Deutschland (IVD) darauf hingewiesen, dass diese Sorgfaltspflicht von Immobilienmaklern bis auf Weiteres nicht im Zusammenhang mit dem Nachweis oder der Vermittlung von Mietverträgen erfüllt werden muss. Allerdings halte ich auch beim Kauf einer Immobilie die Angabe des Geburtsdatums, des Geburtsortes und der Staatsangehörigkeit des Kunden durch den Immobilienmakler erst bei Erklären der Kaufabsicht für erforderlich und nicht bereits bei ersten Anfragen oder der Vereinbarung eines Besichtigungstermins.

Weitere Informationen:

www.lfd.niedersachsen.de > Themen >Wirtschaft > Mieten und Wohnen (Wohnungswirtschaft) Beschluss des Düsseldorfer Kreises vom 22. Oktober 2009: „Bonitätsauskünfte über Mietinteressenten nur eingeschränkt zulässig“ Orientierungshilfe zur „Einholung von Selbstauskünften bei Mietinteressenten“

„Die guten ins Töpfchen, die schlechten ins Kröpfchen“ war einmal: Nutzung bonitätsgeprüfter Adressen für Werbung nicht mehr zulässig

Unternehmen sind nach wie vor sehr daran interessiert, neue Kunden auch über adressierte Werbesendungen gewinnen zu können. Um neue Kundenkreise möglichst zielgenau zu erreichen, sind sie auf aktuelle Adressdaten von solchen potentiellen Kunden angewiesen, die an ihrem Produkt oder ihrer Dienstleistung interessiert sein könnten. Aktives Marketing betreibende Unternehmen greifen daher gerne auf Angebote von Adresshändlern zurück, deren für eine konkrete Werbekampagne vorgesehener Adressbestand bereits um die Daten solcher Personen bereinigt worden ist, deren Bonität unter Berücksichtigung zuvor definierter Kriterien als unzureichend eingeschätzt wird.

Es ist das unter werbeökonomischen Aspekten durchaus nachvollziehbare Ziel der werbenden Unternehmen, von vornherein keine Personen als potentielle Kunden zu bewerben, mit denen sie ohnehin keine Geschäfte abschließen möchten, da anzunehmen ist, dass diese das angebotene Produkt nicht bezahlen können.

Bisherige datenschutzrechtliche Bewertung

„Waschabgleich“: Untersuchung von Adressbeständen mit Hilfe von Auskunfteien unter dem Aspekt der Bonität, um gezielt zahlungskräftige Personen für das jeweils zu bewerbende Produkt ermitteln zu können.

Bisher hat die überwiegende Mehrheit der Datenschutzbehörden den „Waschabgleich“ nicht generell beanstandet, sofern dabei folgendes Verfahren eingehalten wurde:

- Ein Adresshändler lässt im Auftrag eines Unternehmens, das eine Werbeaktion durchführen möchte, die bei ihm vorhandenen Adressbestände nach vorher definierten Bonitätskriterien bei einer Auskunftei oder anhand von Auskunfteidaten bei einem neutralen Dienstleister bereinigen.
- Die bereinigte Adressliste wird dann direkt an einen sogenannten Lettershop weitergeben. Dieser sorgt dafür, dass das Werbematerial, das er von der werbenden Stelle erhalten hat, mit den bereinigten Adressdaten versehen und versandt wird.

Auskunftei: Unternehmen, das unabhängig vom Vorliegen einer konkreten Anfrage geschäftsmäßig bonitätsrelevante Daten über Unternehmen oder Privatpersonen sammelt, um sie bei Bedarf seinen Geschäftspartnern für die Beurteilung der Kreditwürdigkeit des Betroffenen gegen Entgelt zugänglich zu machen. (Ehrmann in Simitis, BDSG, § 29, Rn 84)

Bei diesem Verfahren erhält der Adresshändler die bereinigte Adressliste nicht zurück; ihm werden also keine Bonitätsdaten übermittelt. Auch der Werbetreibende bekommt das Adressmaterial nicht in die Hand. Ihm werden Adressdaten nur bekannt, sofern die über den „Lettershop“-Dienstleister von ihm Umworbenen auf seine Werbeaktion reagieren.

Veränderte Rechtslage führt zu Unzulässigkeit des Verfahrens

Mittlerweile sind sich die Datenschutzbehörden darüber einig, dass dieses Verfahren zur werblichen Nutzung von bonitätsgeprüften Adressen nach heutiger Gesetzeslage aus folgenden Gründen datenschutzrechtlich nicht mehr zulässig ist: Für das zuvor beschriebene Verfahren „bonitätsgeprüfte Adressen“ nutzen Adresshändler und

Auskunfteien ihre Datenbestände, die sie zum Zwecke der Übermittlung nach Maßgabe von § 29 Abs. 1 Bundesdatenschutzgesetz (BDSG) erhoben haben. Über § 29 Abs. 1 Satz 2 BDSG wird hinsichtlich der Datennutzung für werbliche Zwecke auf die Vorschriften des § 28 Abs. 3 BDSG verwiesen, die mittlerweile überwiegend als abschließende Spezialregelung für die Verwendung von Daten für Werbezwecke anerkannt sind.

Dabei gilt für Adresshändler, die von ihnen angebotene Adressdaten nicht für eigene Werbezwecke nutzen, sondern diese vielmehr nur an andere Stellen vermitteln und an der anschließenden werblichen Nutzung nicht beteiligt sind, lediglich § 28 Abs. 3 Satz 1 BDSG[1]. Hiernach ist Adresshandel nur aufgrund einer freiwilligen und informierten Einwilligung des Betroffenen zulässig (siehe auch meinen XX. Tätigkeitsbericht 2009–2010, S. 44). Der in der Vergangenheit häufig praktizierte „Waschabgleich" mit den Auskunftei-Datenbeständen ist daher wegen der aktuellen Rechtslage ohne Einwilligung des Betroffenen nicht mehr zulässig.

Unabhängig davon liegen aber auch die Voraussetzungen des § 28 Abs. 3 Satz 2 BDSG, insbesondere das sogenannte Listenprivileg, im Zusammenhang mit bonitätsgeprüften Adressdaten nicht vor. Der Umstand der geprüften Bonität ist ein für die werbliche Ansprache relevantes Merkmal, das jedoch nicht zu den vom Gesetzgeber genannten Merkmalen einer Adresse gehört, die auch ohne Einwilligung des Betroffenen für werbliche Zwecke genutzt werden dürfen. Auch aus diesem Grund kommt der „Waschabgleich" nunmehr nur noch aufgrund einer Einwilligung des Betroffenen in Betracht.

Letztlich folgt dieses Ergebnis aber auch aus dem Umstand, dass der Gesetzgeber mit der im Jahr 2010 in Kraft getretenen neuen Regelung für Auskunfteien im § 28 a BDSG Sonderregelungen getroffen hat, die eindeutig zum Ziel haben, die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten durch Auskunfteien nur für Bonitätsprüfungszwecke, also zur Vermeidung von Zahlungsausfällen, zuzulassen. Dieser klaren Zweckbindung der von Auskunfteien zulässig vorgehaltenen personenbezogenen Daten würde es jedoch widersprechen, wenn die Bonitätsdaten ohne Einwilligung der Betroffenen auch für einen „Waschabgleich" mit Daten von Adresshändlern herangezogen werden könnten und damit maßgeblich zur Optimierung der Ergebnisse von werblicher Ansprache beitragen würden.

Adrian Ludwig Richter
(1803–1884)
Zeichnung zum Märchen
„Aschenputtel"
(Quelle: Wikipedia)

Auskunfteien wurden informiert

Im Ergebnis haben sich die Datenschutzbehörden aufgrund der inzwischen eingetretenen Rechtsänderungen im BDSG dazu veranlasst gesehen, ihre frühere Einschätzung zur grundsätzlichen Zulässigkeit des „Waschabgleichs" zu revidieren. Die an diesem Verfahren maßgeblich beteiligten Auskunfteien sind über die neue rechtliche Einschätzung zwischenzeitlich informiert worden. Es bleibt abzuwarten, ob Werbewirtschaft und Auskunfteien ihr bisheriges gemeinsames Geschäftsmodell nunmehr der geänderten Rechtslage anpassen werden.

Weitere Informationen:

www.lfd.niedersachsen.de > Themen > Wirtschaft > Handels- und Wirtschaftsauskunfteien

1 s. Wolff/Brink/BeckOK DatenschutzR/Forgó BDSG, Syst. G, 4. BDSG, Rn. 49

Datenschutzverstöße und ihre Konsequenzen: 35 Bußgelder festgesetzt

Auch in 2013 und 2014 führte ich wieder zahlreiche Bußgeldverfahren durch. Den Unternehmen soll so vor Augen geführt werden, dass ein nachlässiger Umgang mit den Datenschutzregelungen nicht geduldet wird.

Im Berichtszeitraum setzte ich insgesamt 35-mal ein Bußgeld fest. Die Einleitung eines Bußgeldverfahrens liegt in meinem Ermessen. Die leitenden Ermessenserwägungen sind dabei unter anderem die Schwere der Tat, der durch den Rechtsverstoß angerichtete Schaden und eine mögliche Uneinsichtigkeit oder Reue des Täters. Erneut lagen die Verstöße überwiegend im Bereich der Auskunftspflichten sowie der Werbung. So ahndete ich

- in elf Fällen einen Verstoß wegen Werbung trotz Vorliegens eines Werbewiderspruchs,
- in acht Fällen einen Verstoß gegen die Verpflichtung zur Auskunftserteilung gegenüber der betroffenen Person und
- immerhin viermal einen Verstoß gegen die Verpflichtung zur Auskunftserteilung gegenüber der Aufsichtsbehörde.

Hier zeigt sich, dass selbst bei solchen offensichtlichen datenschutzrechtlichen Verpflichtungen oft das Gesetz ignoriert wird.
Auch die so genannten Müllfälle traten wieder auf: Hierbei werden Dokumente, die personenbezogene Daten beinhalten, in Altpapiercontainern oder schlicht am Straßenrand entsorgt, so dass Dritte unbegrenzten Zugang erhalten. Hier scheint für einige Unternehmen immer noch die Kostenersparnis durch Verzicht auf datenschutzgerechte Entsorgung schwerer zu wiegen als der Datenschutzgedanke.

Aufsichtspflichtverletzung erstmals geahndet

Im Jahr 2014 habe ich erstmals ein Bußgeld wegen Aufsichtspflichtverletzung im Datenschutzbereich festgesetzt. Dieser Tatbestand ist dann erfüllt, wenn der Inhaber eines Unternehmens es zumindest fahrlässig unterlässt, die erforderlichen Organisations- und Schutzmaßnahmen zu ergreifen und infolgedessen im Unternehmen Rechtsverstöße auftreten (§ 130 OWiG). Die zu ergreifenden Maßnahmen hängen vom Einzelfall und von der Struktur und Arbeitsweise im Unternehmen ab, wesentlich ist aber immer eine ausreichende Instruktion des Personals über Datenschutzvorschriften und deren Durchsetzung sowie eine Organisation des Betriebes dergestalt, dass auch fahrlässige Zuwiderhandlungen gegen Datenschutzrecht möglichst verhindert werden. Insbesondere wenn es bereits zu Unregelmäßigkeiten im Betrieb gekommen ist, sind verstärkte Aufsichtsmaßnahmen zu ergreifen. In dem hier bearbeiteten Vorgang hatte das Unternehmen dies versäumt, und es kam zu weiteren Datenschutzverstößen. Für diese insgesamt mangelhafte Datenschutzorganisation im Unternehmen setzte ich ein empfindliches Bußgeld in Höhe von 5.000 Euro fest.

Überwachung durch GPS-Sender am Fahrzeug

Mehrfach hatte ich mit Vorfällen im Zusammenhang mit einer Überwachung von Personen durch Anbringen eines GPS-Senders an einem Fahrzeug zu tun. Wenn auf diese Weise Mitarbeiter im Betrieb durch Vorgesetzte kontrolliert werden, handelt es sich regelmäßig um einen Verstoß gegen das informationelle Selbstbestimmungsrecht und eine Ordnungswidrigkeit. Entsprechend habe ich erstmals im Berichtszeitraum in zwei Fällen ein Bußgeld wegen einer solchen Überwachung festgesetzt.
Zugenommen haben Anzeigen wegen Ausspionierens von Personen mittels Überwachung ihrer Fahrzeuge durch ihre privaten Ex-Partner. Nach meiner Auffassung unterliegen diese Taten jedoch nicht dem Anwendungsbereich des Bundesdatenschutzgesetzes, da es sich um ein Geschehen innerhalb des privaten Lebensbereiches handelt, welches das Datenschutzrecht nicht durch Regelungen ausfüllen will.

Wiederholungsfälle

Im Berichtszeitraum ist aufgefallen, dass viele Unternehmen und Personen trotz bereits erfolgter „Bestrafung“ durch eine Bußgeldfestsetzung zu einem späteren Zeitpunkt die geahndete Handlung wiederholen. In diesen Fällen habe ich erneute Bußgeldverfahren durchgeführt und die Höhe des Bußgeldes verdoppelt. Viele der Betroffenen zahlen das Bußgeld nicht freiwillig, und es müssen Vollstreckungsverfahren eingeleitet werden. Ich werde dennoch auch künftig Nachlässigkeiten und eine Missachtung des Datenschutzes nicht hinnehmen und Datenschutzverstöße weiterhin mit Bußgeldern ahnden.

7. Beschäftigtendatenschutz

Beschäftigtendatenschutz:
Das rechtliche Niveau muss gehalten werden

Bereits in den beiden vorherigen Tätigkeitsberichten hatte ich die geplanten Neuregelungen zum Beschäftigtendatenschutz dargestellt. Was gibt es also Neues?

Zum Hintergrund: Im Jahr 2009 wurde in das Bundesdatenschutzgesetz (BDSG) mit § 32 eine spezielle Regelung zum Beschäftigtendatenschutz eingefügt. Hiernach darf der Arbeitgeber nur dann Daten des Arbeitnehmers erheben und verarbeiten, wenn dies für die Durchführung des Beschäftigungsverhältnisses objektiv „erforderlich" ist. Es handelt sich bei § 32 BDSG um eine so genannte Generalklausel, so dass diese abstrakte Gesetzesregelung in einer Vielzahl verschiedener Konstellationen zum Beschäftigtendatenschutz ausgelegt und auf den Einzelfall übertragen werden muss. Wie jede Generalklausel überlässt auch § 32 BDSG die konkrete Auslegung dem betroffenen Rechtsanwender und in Streitfällen den Gerichten.
Gesetzliche Konkretisierungen sind jedoch wünschenswert: In einer durch Digitalisierung, Technisierung und globale Datenströme geprägten Arbeitswelt, die immer mehr Möglichkeiten des weltweit erreichbaren, gläsernen Mitarbeiters bietet, kommt dem Beschäftigtendatenschutz eine zunehmende Bedeutung zu. Anders als zum Beispiel bei sozialen Netzwerken, denen man auch ausweichen kann, hat der einzelne Arbeitnehmer nicht die Wahl, sich der Arbeitswelt zu entziehen. Und anders als bei freiwilligen Datenpreisgaben im privaten Bereich (zum Beispiel Unterschriftenlisten in der Fußgängerzone) wird der einzelne Arbeitnehmer bei entsprechendem Druck durch den Arbeitgeber einer „Totalüberwachung in der Firma" oftmals nicht widersprechen, da er sich aus Angst um den Arbeitsplatz nicht traut, seine Rechte gegenüber dem Arbeitgeber wahrzunehmen.

Überwachung durch Datenbrillen, Biometrie, GPS-Handys

Als konkrete Beispiele für diese neuartigen Szenarien sind Datenbrillen bei Lagerarbeitern, der zunehmende Einsatz biometrischer Verfahren in Firmen oder GPS-Handys für Hausmeister zu nennen. Angesichts dieser neuen Herausforderungen spricht viel dafür, dass es über die erwähnte Generalklausel hinaus Spezialregelungen des Gesetzgebers bedarf, welche die konkreten Grundentscheidungen zugunsten der Beschäftigten auf eine gesetzliche Grundlage stellen. Diese Forderung ist nicht neu: Bereits 2010, also ein Jahr nach Erlass der erwähnten Generalklausel, brachte die Bundesregierung detaillierte Regelungen zum Beschäftigtendatenschutz, als geplanten Unterabschnitt des Bun-

desdatenschutzgesetzes, in das Gesetzgebungsverfahren ein. Hierauf bezog sich eine Entschließung der Datenschutzkonferenz des Bundes und der Länder vom März 2011, in der ich zusammen mit meinen Kolleginnen und Kollegen Nachbesserungen forderte. Als das Gesetzgebungsvorhaben dann zwei Jahre später von den Koalitionspartnern mit umfassenden Änderungen in den Innenausschuss des Bundestages eingebracht wurde, wies die Datenschutzkonferenz im Januar 2013 in einer weiteren Entschließung darauf hin, dass zwar einige datenschutzrechtliche Forderungen zwischenzeitlich aufgegriffen worden seien, aber in anderen Bereichen das Datenschutzniveau für die Beschäftigten durch die eingebrachte Novellierung noch weiter abgesenkt werde. Nachdem unter anderem auch der DGB gegen den Gesetzesentwurf „Sturm gelaufen war", wurde das Thema noch im Januar 2013 von der Tagesordnung des Innenausschusses sowie des Bundestages genommen.

Forderungen der Datenschutzbeauftragten aktueller denn je

Wie ist nun der aktuelle Stand? Nach der Bundestagswahl im September 2013, also in der 18. Legislaturperiode, nahmen CDU, CSU und SPD den Beschäftigtendatenschutz in ihren Koalitionsvertrag auf. Hierbei bekannten sich die Regierungsparteien dazu, das Niveau des deutschen Beschäftigtendatenschutzes bei den Verhandlungen zur Europäischen Datenschutzgrundverordnung zu erhalten. Zugleich wurde vereinbart, dass – sollte die Europäische Datenschutzgrundverordnung nicht in absehbarer Zeit vorliegen – eine nationale Regelung zum Beschäftigtendatenschutz geschaffen werden soll. In einer dritten Entschließung stellte ich gemeinsam mit meinen Kolleginnen und Kollegen der Datenschutzaufsichtsbehörden des Bundes und der Länder im März 2014 klar, dass die gemäß Koalitionsvertrag „offene Zeitschiene" nicht ausreiche. Angesichts der voranschreitenden technischen Entwicklung forderten wir die Bundesregierung auf, ein nationales Beschäftigtendatenschutzgesetz umgehend auf den Weg zu bringen. Hierbei stellten wir klar, dass weiterhin ein hohes Datenschutzniveau gewährleistet sein müsse.
Unabhängig davon, ob die Verhandlungen zur Europäischen Datenschutzgrundverordnung zeitnah zum Abschluss gebracht werden oder in der Grundverordnung verbindliche europaweite Regelungen zum Beschäftigtendatenschutz enthalten sein werden, gilt Folgendes: Für den einzelnen Arbeitnehmer, der sich mit einer Petition an meine Behörde wendet, ist allein relevant, dass das Niveau des Datenschutzrechts in Deutschland – bei weiterhin fortschreitender Technisierung – zumindest gleichbleibt. Dies kann nur durch entsprechende nationale Regelungen, die zeitnah eingebracht werden, garantiert werden. Die Forderungen der Entschließung vom März 2014 sind daher aktueller denn je.

Weitere Informationen:

Entschließungen der Datenschutzkonferenz unter www.lfd.niedersachsen.de > Allgemein > DSB-Konferenzen > Entschließungen

Weitergabe von Arbeitnehmerdaten: Datenübermittlung an Agrar-Zertifizierungsstellen rechtswidrig

Private Zertifizierungssysteme können für Firmen eine Chance im Wettbewerb sein. Was aber, wenn sie in Widerspruch zum Beschäftigtendatenschutz stehen? Ein Obstanbauer trug einen solchen Sachverhalt an mich heran.

Gegenstand seiner Petition war ein Agrar-Zertifizierungssystem. Er schilderte folgenden Hintergrund: Lokale Obst-Landwirte sind oftmals von einem bestimmten Zwischenhändler oder von einer einzelnen Lebensmittelkette abhängig. Diese einzelnen Großhändler setzen zunehmend auf bestimmte Zertifizierungssysteme, um weltweit einheitliche Standards zu gewährleisten. Im konkreten Fall ging es nun um eines der weltweit größten privatrechtlich organisierten Zertifizierungssysteme, das in zirka 100 Ländern anerkannt ist. Hierbei werden neben der Lebensmittelqualität und der Umweltverträglichkeit der Herstellung auch Sozialkriterien bewertet, also wie die Arbeitnehmer am Arbeitsplatz behandelt werden.

Detaillierte Arbeitnehmerdaten

Vor diesem Hintergrund verlangte nun der Großhändler vom Petenten, dass dessen Obsthof das Zertifizierungsverfahren absolviert. Als Teil des Zertifizierungsverfahrens sollten zahlreiche Detaildaten zu sämtlichen auf dem Obsthof beschäftigten Arbeitnehmern an die nationale und dann auch globale Zertifizierungsstelle („zur Aufnahme in die Global-Datenbank“) übermittelt werden. Zu den abverlangten Daten gehörten unter anderem die Kategorien

- Vorname, Nachname,
- Beginn des Dienstverhältnisses, gegebenenfalls vereinbartes Ende des Dienstverhältnisses,
- Lohnkategorie laut Arbeitsvertrag,
- vereinbarter Bruttolohn,
- vereinbarte Arbeitszeiten und
- geleistete Arbeitszeiten der einzelnen Beschäftigten.

Als mögliches Mittel war auch eine Einsichtnahme in den Arbeitsvertrag vorgesehen. Zwar ist in den Zertifizierungsunterlagen auch erwähnt, dass eine Einwilligung der Arbeitnehmer erforderlich ist und dass bei deren Verweigerung der Einwilligung auch eine anonymisierte Übermittlung der Arbeitnehmerdaten möglich ist. Gleichwohl wird faktisch über das Zertifizierungssystem ein hoher Druck auf die Landwirte und damit auch auf ihre Beschäftigten ausgeübt, die Daten zu übermitteln. Denn nicht zertifizierte Landwirtschaftsbetriebe sehen sich der konkreten Drohkulisse ausgesetzt, ohne Zertifi-

zierung nicht mehr von Großhändlern gelistet zu werden. Nicht zertifiziert zu sein, kann also eine Markteintrittsbarriere darstellen.

Kein nachvollziehbarer Zweck erkennbar

Die Rechtslage ist hingegen eindeutig: Die Datenanforderung wäre nur dann rechtmäßig, wenn dies gemäß § 32 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG) für die Durchführung des Beschäftigungsverhältnisses erforderlich wäre. Es ist jedoch nicht annähernd ein nachvollziehbarer Zweck für eine solche Übertragung von Beschäftigtendaten an Dritte erkennbar. Der Druck auf den Landwirt durch den Großhändler ist für die Erforderlichkeit im bilateralen Verhältnis Arbeitgeber – Beschäftigter irrelevant, da der Beschäftigte auch ohne die Datenübertragung seine Arbeitsleistung voll erbringen kann. Die wirtschaftliche Situation (drohendes Ausbleiben von Aufträgen) spielt daher für die Rechtsfrage der Erforderlichkeit keine Rolle. Die Erforderlichkeit gemäß § 32 Abs. 1 S. 1 BDSG ist daher zu verneinen. Auch andere Rechtsgrundlagen, insbesondere § 28 BDSG, kommen nicht in Betracht. Eine wirksame Einwilligung des Beschäftigten ist gemäß § 4 a Abs. 1 S. 1 BDSG ebenfalls ausgeschlossen, da der Beschäftigte im Über-/Unterordnungsverhältnis des Arbeitsvertrags im Zweifel dem Druck nachgeben wird und somit nicht autonom (wie im privaten Bereich) entscheiden kann.

In der vorliegenden Konstellation konnte ich dem Petenten daher mitteilen, dass es für die erbetene Datenübertragung keine Rechtsgrundlage gibt, sie wäre daher rechtswidrig.

Biometrisches Zugangssystem: Fingerabdruckscanner in Fensterfirma unzulässig

Zum Stichwort Fingerabdruckscanner erreichte mich eine Anfrage einer Firma, die im Internet mit Holzfenstern handelt. Das Unternehmen hat ungefähr 50 Mitarbeiter. In der Firma wurde der Einsatz eines biometrischen Zugangssystems mittels Fingerabdruck geplant. Ich wurde gebeten, die rechtliche Zulässigkeit zu beurteilen.

Ob Mitarbeiterdaten erhoben werden dürfen, richtet sich nach § 32 Bundesdatenschutzgesetz (BDSG). Hiernach ist relevant, ob die Erfassung des Fingerabdrucks erforderlich ist zur Durchführung des jeweiligen Beschäftigungsverhältnisses. Auf Details zu den Erhebungsdaten (wird zum Beispiel im Ergebnis nur ein mathematischer Wert abgeglichen oder werden tatsächlich biometrische Merkmale der Beschäftigten dauerhaft gespeichert?) kam es in diesem konkreten Einzelfall nicht entscheidend an. Vielmehr war entscheidend, ob ein solches System selbst bei geringer Eingriffstiefe erforderlich ist. Für die Erfassung derart sensibler Daten ist die Erforderlichkeit nur dann zu bejahen, wenn es sich um Branchen handelt, bei denen Sicherheitsaspekte eine große Rolle spielen, insbesondere bezogen auf Leib und Leben wie in einem Hochsicherheitslabor oder auf besonders hohe Wertbeträge wie im Tresorbereich.

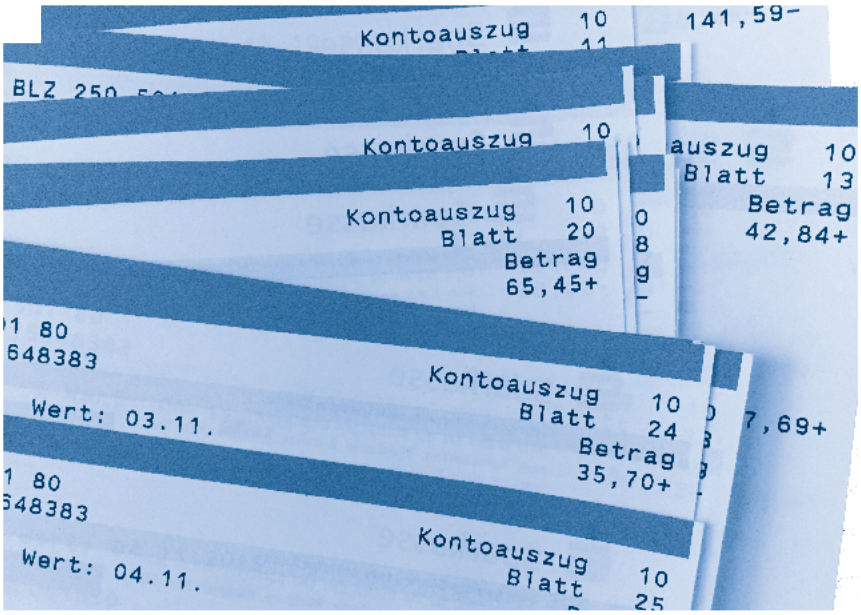
Zweck auch mit Chipkarte oder Passwort erreichbar

Die anfragende Firma, die im Internet handelsübliche Fenster verkauft, hatte dagegen kein sicherheitsrelevantes Tätigkeitsgebiet; es bestand kein Unterschied zu anderen, „normalen“ Firmen. Der beabsichtigte Zweck (Zugangskontrolle) konnte daher auch mit einer Chipkarte oder einem Passwort sichergestellt werden, zumal sich die rund 50 Mitarbeiter jeweils persönlich kennen dürften. Auch das vorgebrachte Argument, dass eine Chipkarte vergessen werden könne, war nicht stichhaltig: Bei Vergessen der Chipkarte kann der jeweilige Mitarbeiter zum Beispiel mit einer Besucherchipkarte ausgestattet werden.
Ich konnte der Firma daher die Antwort mitteilen, dass für eine Erhebung biometrischer Daten keine Erforderlichkeit besteht; eine solche Datenerhebung wäre daher rechtswidrig. Auch bei Firmen mit erhöhter Sicherheitsrelevanz sind allerdings immer noch Zwischenlösungen möglich. Beispielsweise kann ein Schutz vor Spionage auch sichergestellt werden durch die Kombination von Chipkarte und zusätzlichem Passwort. Alternativ wäre denkbar, nur sensible Bereiche wie Entwicklungsabteilungen für die dort Beschäftigten mit einem Fingerabdrucksystem auszustatten. Eine pauschale Anwendung auf alle Beschäftigten wäre jedoch auch in solchen Fällen nicht erforderlich.

Konto beim Arbeitgeber: Bank darf nicht Mitarbeiterkonten einsehen

Ein Arbeitgeber darf grundsätzlich keine Kontodaten seiner Mitarbeiter erheben. Was aber ist, wenn die kontoführende Bank des Kunden gleichzeitig dessen Arbeitgeber ist?

Um diese Konstellation ging es bei einer Rechtsberatung. Ein Mitarbeiter eines Bankhauses, der bei dieser Bank zugleich sein Konto führte, wurde von einem Leitenden Angestellten auf regelmäßige Geldeingänge auf seinem Konto angesprochen. Vom Rechenzentrum der Bank sei ein Einblick in die Konten der Mitarbeiter möglich; Hintergrund der Frage seien Aspekte der Bestechlichkeit bzw. einer unerlaubten Nebentätigkeit. Der Petent war über diese Anfrage des Leitenden Angestellten erstaunt und suchte rechtliche Beratung.
Ich teilte dem Petenten mit, dass ein solcher Zugriff auf die Kontoübersichten der Mitarbeiter durch die Arbeitgeber-Bank rechtswidrig sei. Eine Rechtsgrundlage für eine solche Datenerhebung besteht nicht. Vielmehr sind die zwei verschiedenen Vertragsverhältnisse (Arbeitsverhältnis einerseits/Kontoführungsverhältnis andererseits) strikt zu trennen. Die Bank hat somit keine weitergehenden Rechte als andere Arbeitgeber.



8. Videoüberwachung

Kameras in Bussen und Bahnen: Unternehmen streben Totalüberwachung an

Videoüberwachung hat mittlerweile in Bussen und Bahnen des öffentlichen Personennahverkehrs (ÖPNV) und des schienengebundenen Regionalverkehrs (SPNV) fast flächendeckend Einzug gehalten. Der zwischen dem Düsseldorfer Kreis, dem Aufsichtsgremium der Datenschutzbeauftragten von Bund und Ländern für den nicht-öffentlichen Bereich, und dem Verband Deutscher Verkehrsunternehmen (VDV) im Jahr 2001 abgestimmte Grundsatz der Einzelfallprüfung findet daher mittlerweile faktisch keine Anwendung mehr.

Dabei erfolgt die Videoüberwachung in erster Linie zur Verbesserung des Sicherheitsgefühls der Fahrgäste und zur Vermeidung und Verfolgung von Vandalismusschäden in den Fahrgastbereichen der Fahrzeuge. Es geht also um die Abschreckung von Straftätern sowie um die Dokumentation von Straftaten mit dem Ziel, diese besser verfolgen zu können. Einige ÖPNV-Unternehmen nutzen die Videoüberwachung darüber hinaus auch, um etwaige Schadenersatzansprüche ihrer Kunden wegen Verletzung von Verkehrssicherungspflichten abzuwehren. Zur Erreichung dieser Ziele streben die Verkehrsunternehmen eine sowohl räumlich wie auch zeitlich möglichst umfassende Erfassung des gesamten Fahrgastbereichs des jeweiligen Verkehrsmittels mit Kameras an.
Ein solch umfassendes Einsatzkonzept von Videoüberwachungskameras in öffentlichen Verkehrsmitteln wirft zwangsläufig die Frage nach dessen datenschutzrechtlichen Grenzen auf. Die mit der Videoüberwachung verfolgten Ziele stehen nämlich im Spannungsverhältnis zum Recht eines jeden Menschen, sich in der Öffentlichkeit frei bewegen zu können, ohne dass sein Verhalten permanent von Kameras beobachtet oder aufgezeichnet wird.

Gebot der Datensparsamkeit missachtet

Problematisch ist dabei insbesondere der Ansatz im ÖPNV/SPNV, dass zum Beispiel die Landesnahverkehrsgesellschaft Niedersachsen (LNVG) schon seit einiger Zeit im Rahmen ihrer Ausschreibungen von Verkehrsleistungen generell eine zwar datenschutzkonforme, aber im Widerspruch dazu dennoch über 90 Prozent des Fahrgastraumes erfassende Videoüberwachung fordert. Damit verlangt die LNVG von den Unternehmen, die letztlich die beauftragten Verkehrsleistungen erbringen, diese Forderungen uneingeschränkt umzusetzen. Die LNVG unterstützt ihre Forderung zudem dadurch,

dass sie in der Regel den Verkehrsunternehmen auch die mit entsprechender Videotechnik ausgestatteten Fahrzeuge zur Verfügung stellt. Eine über 90 Prozent der Fahrgastbereiche abdeckende Videoüberwachung ist aber gerade nicht datenschutzgerecht, sondern widerspricht eindeutig dem Gebot der Datenvermeidung und Datensparsamkeit (§ 3 a BDSG) und ist unverhältnismäßig[1]. Insbesondere ist aber auch problematisch, dass ein Neuausrichten der Kameras nicht möglich ist und die Software das Einrichten von Privatzonen nicht unterstützt. Diese Probleme wurden auch bei meinen Prüfungen verschiedener Verkehrsunternehmen im Berichtszeitraum deutlich.

Trotz der von den geprüften Verkehrsunternehmen immer wieder vorgebrachten Sicherheitsargumente kann auch im ÖPNV/SPNV eine Videoüberwachung nur zulässig sein, wenn

- eine Gefahrenlage nachgewiesen ist, die ein **berechtigtes Interesse** an der Videoüberwachung dem Grunde und dem Umfang nach zu begründen vermag,
- eine Videoüberwachung **erforderlich i**st und
- die **Interessen der Betroffenen** nicht überwiegen.

Berechtigtes Interesse:

Es sind konkrete Tatsachen zu fordern, aus denen sich eine Gefährdung ergibt, beispielsweise Beschädigungen oder besondere Vorkommnisse in der Vergangenheit (z. B. Missbrauch von Notbrems- oder Notrufeinrichtungen). Das in diesem Kontext maßgebende berechtigte Interesse i.S.d. § 6 b Abs.1 Nr.3 BDSG liegt demnach jedenfalls dann nicht vor, wenn die Überwachung in den Fahrzeugen lediglich mit dem Ziel einer allgemeinen und abstrakten Gefahrenvorsorge begründet wird. Davon ist jedoch auszugehen, wenn neue Fahrzeuge mit umfassender Videoüberwachungsausstattung alte Fahrzeuge ohne entsprechende Ausstattung ersetzen und der Betrieb der alten Fahrzeuge ohne Videoüberwachung bislang problemlos möglich war.

1 So auch Simitis/Scholz, Kommentierung zum BDSG, 8. Auflage, § 6 b, Rdnr. 95

Erforderlichkeit:
Sie ist nur dann beachtet, wenn die Überwachung geeignet ist, um das festgelegte Ziel zu erreichen. Soll die Videoüberwachung z. B. rein präventiven Zwecken dienen, ist eine Beobachtung des Geschehens über Monitore („Monitoringmodus"), so wie es § 6 b Abs. 1 BDSG voraussetzt, erforderlich aber auch ausreichend[2]. Unabhängig davon ist die Videoüberwachung nur dann erforderlich, wenn es kein milderes, in die Rechte der Betroffenen weniger einschneidendes Mittel gibt. Vor dem Einsatz von Kameras müssen sich deshalb die Verkehrsunternehmen mit zumutbaren alternativen Methoden auseinandersetzen, die in das Persönlichkeitsrecht der Fahrgäste weniger eingreifen. So kann der regelmäßige Einsatz von Personal dem Schutzbedürfnis der Fahrgäste ebenso gut, wenn nicht sogar besser Rechnung tragen als der Einsatz von Überwachungskameras, die bei einer reinen Black-Box-Aufzeichnungslösung ohnehin keinen präventiven Fahrgastschutz bieten können. Auch die Verwendung besonders widerstandsfähiger Sitze und Sitzbezüge sowie eine spezielle Oberflächenbeschichtung können Vandalismusschäden vorbeugen. Zudem kann eine zeitlich begrenzte Überwachung (z. B. nur zu bestimmten Tages- oder Nachtzeiten) oder der Kameraeinsatz nur auf besonders gefährdeten Linien oder beschränkt auf schlecht einsehbare Fahrgastbereiche ausreichen und so zur Wahrung der berechtigten Interessen der von der Videoüberwachung betroffenen Fahrgäste beitragen. In allen anderen Fällen müssen installierte Kameras im Übrigen ausgeschaltet bleiben; zur Herstellung von Transparenz sollte dies zudem mit einem entsprechenden LED-Signal am Kameragehäuse kenntlich gemacht werden.

Interessen der Betroffenen:
Auch wenn ein berechtigtes Interesse des Unternehmens und die Erforderlichkeit gegeben sind, ist eine Abwägung des Firmeninteresses mit dem Interesse des betroffenen Fahrgastes, von der Überwachung möglichst verschont zu bleiben, vorzunehmen. Maßstab der Bewertung ist das informationelle Selbstbestimmungsrecht des Fahrgastes auf der einen Seite und der Schutz des Eigentums und des Personals des Betreibers auf der anderen. Dabei darf die Intensität der Grundrechtsbeschränkung aufgrund der Überwachungsmaßnahme nicht außer Verhältnis zu dem Gewicht des Überwachungsinteresses stehen. So stellt die permanente, lücken- und vor allem verdachtslose Überwachung des Fahrgastraumes, der sich der Fahrgast nicht entziehen kann, einen weiterreichenden Eingriff dar als eine nur zeitweilige Beobachtung, die nur Teilbereiche des Raumes erfasst[3]. Dasselbe gilt hinsichtlich der typischen Aufenthaltsdauer im Verkehrsmittel: je länger der Beförderungsvorgang, desto höher sind die schutzwürdigen Interessen des Fahrgastes zu gewichten. Sind keine überwachungsfreien Zonen vorgesehen, bestehen regelmäßig Anhaltspunkte für ein Überwiegen schutzwürdiger Interessen der betroffenen Fahrgäste. Dies gilt insbesondere für die Überwachung von Sitzplatzbereichen. Toiletten und vergleichbare weitere Sanitärräume in Fahrzeugen müssen stets überwachungsfrei bleiben.
Bei meinen Prüfungen musste ich feststellen, dass die genannten Voraussetzungen für eine zulässige Videoüberwachung weitgehend nicht beachtet wurden.

Keine Zahlen vorgelegt, keine Interessenabwägung durchgeführt

Der Nachweis einer Gefahrenlage durch Vorlage von belastbaren Daten zu vorangegangenen Vorfällen konnte nicht oder nicht ausreichend erbracht werden. Sofern Vorfälle dokumentiert waren, konnten die Unternehmen nicht angeben, ob die Videoüberwachung zur Aufklärung

2 Simitis/Scholz, a.a.O., Rdnr. 90
3 BVerfG, Beschluss vom 23. Februar 2007, DVBl 2007, 501 f.

dieser Vorfälle hatte beitragen können. Die Interessenabwägung war regelmäßig unterblieben. Stattdessen konfrontierten mich die Verkehrsunternehmen mit dem Argument – es ist inzwischen ihr Hauptargument –, die Videoüberwachung diene der Befriedigung des Schutzbedürfnisses der Fahrgäste. Auf das Fehlen der Interessenabwägung hingewiesen, beschränkten und beschränken sich die Unternehmen weitgehend auf die Behauptung, die Überwachung werde von den Fahrgästen selbst gewünscht. Dabei verkennen die Verkehrsunternehmen, dass der Zweck des präventiven Fahrgastschutzes in der Regel nur mit der Wahrnehmung des Hausrechtes, also dem Schutz des Objekts und der sich darin aufhaltenden Personen gerechtfertigt werden kann. Das Hausrecht kann jedoch mit dieser präventiven Zielsetzung nur wirksam ausgeübt werden, wenn bei einem Verstoß direkt eingegriffen werden kann, also zum Beispiel Polizei oder Krankenwagen alarmiert werden können. Eine Videoüberwachung, die dem Schutzbedürfnis der Fahrgäste dienen soll, kann daher effektiv nur im Monitoringmodus einschließlich einer Interventionsmöglichkeit betrieben werden (siehe auch Beitrag „Videoüberwachung in Einkaufspassage“ auf Seite 103 zum konzeptionell sinnvollen und datenschutzrechtlich vertretbaren Videoeinsatz).

Nur dort, wo die Livebilder auf einem Monitor beobachtet und bei Bedarf eigene Sicherheitskräfte oder die Polizei alarmiert werden, darf im Falle eines Übergriffs tatsächlich auf Hilfe gehofft werden.

Zwei der überprüften Unternehmen speicherten die Videodaten jedoch lediglich im sogenannten Black-Box-Verfahren, das Auslesen erfolgte nur auf Verlangen der Polizei. Die Daten konnten somit allenfalls nach einer begangenen Straftat als Beweise gegen mutmaßliche Täter dienen. Hier wird die Ungeeignetheit des Überwachungskonzeptes besonders deutlich. Denn Betroffene dürfen im Falle eines Übergriffs nur dann auf Hilfe hoffen, wenn Livebilder auf einem Monitor beobachtet und bei Bedarf Sicherheitskräfte des Unternehmens oder die Polizei alarmiert werden.

Empfehlung in Vorbereitung

Die gegen die Verkehrsunternehmen eingeleiteten datenschutzrechtlichen Prüfungen, die sich wegen ihrer Komplexität über einen längeren Zeitraum erstrecken, sind noch nicht beendet, so dass ich voraussichtlich erst in meinem nächsten Tätigkeitsbericht abschließend über die Ergebnisse werde berichten können. Allerdings erhoffe ich mir eine Beschleunigung auch künftiger Prüfverfahren in diesem Bereich von dem Umstand, dass die Datenschutzbeauftragten des Bundes und der Länder derzeit eine Empfehlung für die Verkehrsunternehmen zum datenschutzgerechten Einsatz von optisch-elektronischen Einrichtungen in Verkehrsmitteln erarbeiten, die voraussichtlich im Jahr 2015 verabschiedet werden wird.

Weitere Informationen:

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ unter www.lfd.niedersachsen.de > Themen > Videoüberwachung > Videoüberwachung durch private Stellen und Unternehmen

Die Datenschutzbeauftragte empfiehlt: Finger weg von Dashcams

Einer weit verbreiteten Meinung zufolge sind 99 Prozent der Autofahrer der festen Überzeugung, dass alle anderen Verkehrsteilnehmer nicht Auto fahren können, weshalb es selbstverständlich geboten zu sein scheint, sich vor diesen Mitmenschen im Straßenverkehr zu schützen. Kein Wunder also, dass der Einsatz von Dashcams in letzter Zeit deutlich zugenommen hat.

Dashcams (abgeleitet aus dash board, also Armaturenbrett, und camera) sind Videoaufnahmegeräte, die im Handel verharmlosend meist als „Action-Cam" angeboten werden und die an der Windschutzscheibe, der Heckscheibe oder auf dem Armaturenbrett eines Kraftfahrzeugs befestigt werden. Sie werden zumeist dazu genutzt, um während der Fahrt permanent den Straßenverkehr aufzuzeichnen und um im Fall eines Unfalls ein Beweismittel zur Hand zu haben.
Dass die Nutzung einer solchen Kamera bei den davon betroffenen anderen Verkehrsteilnehmern auf wenig Verständnis stößt, ist ohne weiteres nachvollziehbar. Und so haben mich im Berichtszeitraum einige solcher Fälle beschäftigt, die mir zumeist von der Polizei zur datenschutzrechtlichen Beurteilung vorgelegt wurden. Daneben hatte ich mich aber auch mit dem besonderen Fall eines Autofahrers zu befassen, der es sich zur Aufgabe gemacht hat, in großem Umfang das vermeintlich oder tatsächlich verkehrswidrige Verhalten anderer Verkehrsteilnehmer mit Dashcam-Aufnahmen aus dem eigenen Fahrzeug zu dokumentieren und diese als Beweismittel für anschließende Verkehrsordnungswidrigkeitsanzeigen zu nutzen, ohne dass der Anzeige erstattende Autofahrer jedoch persönlich durch das vermeintlich verkehrswidrige Verhalten eingeschränkt worden war.

Alle Verkehrsteilnehmer unter Generalverdacht

Bereits in meinem XXI. Tätigkeitsbericht habe ich mich zur Zulässigkeit von Dashcams unter dem Gesichtspunkt der „Videoüberwachung in und an Taxis sowie an privaten Kfz" geäußert und darauf hingewiesen, dass der Betrieb von Außenkameras als sogenannte Unfallkameras weder in Taxis noch in privaten Kfz zulässig ist. Wesentlicher Grund für diese klare datenschutzrechtliche Einschätzung war und ist der Umstand, dass Dashcams den Verkehr sowie Personen, die sich in der Nähe einer Straße aufhalten, ohne Anlass und permanent aufzeichnen, so dass eine Vielzahl von Verkehrsteilnehmern betroffen ist, die sämtlich unter einen Generalverdacht gestellt werden, ohne dass sie von der Überwachung Kenntnis erlangen oder sich dieser entziehen können. Das Interesse des Autofahrers, für den eher theoretischen Fall eines Verkehrsunfalls Videoaufnahmen als Beweismittel zur Hand zu haben, kann diesen gravierenden Eingriff in das Persönlichkeitsrecht der Verkehrsteilnehmer nicht rechtfertigen. Daher liegen die Voraussetzungen des hier alleine in Betracht kommenden § 6 b Bundesdatenschutzgesetz (BDSG) für die zulässige Videoüberwachung öffentlich zugänglicher Räume auch dann nicht vor, wenn man in der Dashcam-Nutzung überhaupt die Wahrnehmung eines berechtigten Interesses i.S.d. § 6 b Abs.1 Nr. 3 BDSG sehen will.
Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) haben deshalb in einem Beschluss vom 25./26. Februar 2014 nochmals die Unzulässigkeit jeglicher Videoüberwachung aus Fahrzeugen mittels Dashcams unterstrichen. Diese Position der Aufsichtsbehörden hat sich auch der Niedersächsische Minister für Inneres und Sport, Boris Pistorius, anlässlich der Beantwortung einer Kleinen Anfrage am 11. September 2014 zu eigen gemacht (LT-Drs 17/1998).

Gerichte: Permanente Überwachung des Straßenverkehrs rechtswidrig

Inzwischen gibt es darüber hinaus erste Gerichtsentscheidungen zu dieser Thematik, die die mittlerweile gefestigte Position der Datenschutzbehörden bestätigen. So hat das Verwaltungsgericht Ansbach in seinem rechtskräftigen Urteil vom 12. August 2014 (AN 4 K 13.01634) festgestellt, dass der permanente Einsatz einer Dashcam zu dem Zweck, die Aufnahmen im Falle einer Verwicklung des Nutzers der Dashcam in verkehrsrechtliche Streitigkeiten oder in einen Unfall an die Polizei weiterzugeben oder in einem Schadensersatzprozess als Beweismittel zu verwenden, nach dem BDSG nicht zulässig ist. Maßgebend hierfür ist nach Ansicht des Gerichtes, dass das BDSG heimliche Aufnahmen unbeteiligter Dritter grundsätzlich nicht zulässt und solche Aufnahmen einen erheblichen Eingriff in das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung der von den Filmaufnahmen betroffenen Personen darstellen. Das Interesse dieser Personen überwiege deshalb das geltend gemachte Interesse des Klägers an der Fertigung von Aufnahmen mit einer Dashcam.
Auch das Amtsgericht München hat sich dieser Ansicht angeschlossen und mit Beschluss vom 13. August 2014, Az. 345 C 5551/14, festgestellt, dass die permanente, anlasslose Überwachung des Straßenverkehrs durch eine in einem PKW installierte Autokamera gegen § 6 b Abs. 1 Nr. 3 BDSG sowie gegen § 22 S. 1 Kunsturhebergesetz (KunstUrhG) verstößt und den Betroffenen in seinem Recht auf informationelle Selbstbestimmung als Ausfluss seines allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1, 1 Abs. 1 GG verletzt. Im Ergebnis können die Aufzeichnungen aus einer Dashcam nach diesem Richterspruch auch im Zivilprozess nicht als Beweismittel verwertet werden.
Zu demselben Ergebnis ist auch das Landgericht Heilbronn (Urteil vom 17. Februar 2015 – Az.: I 3 S 19/14) gelangt und hat ergänzend festgestellt:
„Wollte man dies anders sehen und der bloßen Möglichkeit, dass eine Beweisführung erforderlich werden könnte, den Vorrang vor dem Recht auf informationelle Selbstbestimmung einräumen, würde dies bedeuten, dass innerhalb kürzester Zeit jeder Bürger Kameras befestigen würde, um damit zur Dokumentation und als Beweismittel zur Durchsetzung von möglichen Schadensersatzansprüchen jedermann permanent zu filmen und zu überwachen. Damit aber würde das Recht auf informationelle Selbstbestimmung praktisch aufgegeben.“ Diesen klaren und die Bedeutung des Datenschutzes angemessen würdigenden Aussagen des Landgerichts Heilbronn schließe ich mich uneingeschränkt an. Ich werde – wie in dem eingangs geschilderten Fall des Anzeigen erstattenden Autofahrers geschehen – auch künftig in Fällen, in denen wiederholt Dashcams zur Dokumentation von Straftaten, Verkehrsordnungswidrigkeiten oder eines Unfallhergangs einsetzt werden, ein Bußgeldverfahren wegen unbefugter Datenerhebung und -verarbeitung (§ 43 Abs. 2 Nr. 1 BDSG) einleiten sowie nötigenfalls den Dashcam-Einsatz durch Erlass einer Anordnung nach § 38 Abs.5 BDSG unterbinden.

Weitere Informationen:

www.lfd.niedersachsen.de > Themen > Video- überwachung > Videoüberwachung durch private Stellen und Unternehmen

Kameras im Schlachthof: Für Hygieneschleuse erlaubt, für Stempeluhr nicht

Überwachungskameras hängen überall, selbst in Schlachthöfen. Ich hatte daher Anlass, im Berichtszeitraum auch die Videoüberwachung in zwei Betrieben der fleischverarbeitenden Lebensmittelindustrie zu prüfen. Auslöser waren jeweils Eingaben, einerseits aus dem Kreis der Beschäftigten und andererseits aus der Gruppe von Bürgerinitiativen, die aus Immissions- oder Tierschutzgründen gegen Großschlachtbetriebe mit vielfältigen Aktionen vorgehen.

Gegenstand meiner Tätigkeit war sowohl die Beratung zu geplanten Einsatzkonzepten für Überwachungskameras als auch die Prüfung bereits bestehender Überwachungen im Rahmen eines Kontrollverfahrens. Meine Zuständigkeit ist dabei nur gegeben, wenn personenbezogene Daten erfasst werden, nicht aber, wenn es um Videoüberwachung geht, die zur Einhaltung tierschutzrechtlicher Regelungen beim Schlachten von Rindern, Hühnern und Schweinen durchgeführt wird. Auch die im Rahmen der Vor-Ort-Kontrollen angetroffenen Wärmebildkameras, die zur nächtlichen Absicherung des eingezäunten Betriebsgeländes eingesetzt werden, unterliegen nicht dem Bundesdatenschutzgesetz (BDSG), da mit ihnen keine personenbezogenen Daten im Sinne des § 3 Abs. 1 BDSG erhoben werden.

Mitarbeiterschutz in der Gitterbox

Neben der Überwachung des tierschutzgerechten Schlachtbetriebs wurde die Videoüberwachung aber auch zum Nachweis der Beachtung von Hygienevorschriften eingesetzt. Bei derartigen Überwachungen ist unbedingt § 32 Abs. 1 Satz 2 BDSG zu beachten, welcher die Videoüberwachung im Beschäftigungsverhältnis regelt. Konkret war hier beispielsweise die Überwachung einer Gitterbox unzulässig, die für Schlachtpersonal zugänglich ist, und in der das hochwertige Schlacht- und Zerlegebesteck aufbewahrt wird. Die Videoüberwachung der Hygieneschleuse war im Rahmen der Lebensmittelsicherheit grundsätzlich zulässig, allerdings war der Erfassungsbereich der Kameras auf die Schleuse zu beschränken. Eine darüber hinausgehende Videoüberwachung wäre bereits mangels Erforderlichkeit unzulässig. Bei den Prüfungen stellte ich aber fest, dass neben einer zulässigen Überwachung der Einhaltung der Hygienevorschriften gleichzeitig eine Beobachtung der benachbarten Stempeluhr erfolgte, was datenschutzrechtlich und unter Berücksichtigung der ständigen Rechtsprechung des Bundesarbeitsgerichts unzulässig ist.
Eine im Rahmen meiner Prüfungen begutachtete Videoüberwachung in der Produktion beurteilte ich trotz der dort vorhandenen Arbeitsplätze für Zerlegepersonal als zulässig, da diese ohne Aufzeichnung als reine Beobachtung (Monitoring) des überwiegend automatisierten Produktionsablaufs erfolgt und diese Bilder auch nur auf einem Monitor im Bereich der Produktionssteuerung auflaufen und nicht von anderen Bereichen wie der Security im Pförtnerbüro eingesehen werden. Die auch hier gebotene Abwägung

zwischen den mit dem Kameraeinsatz verfolgten Tierschutz- und seuchenhygienischen Zielen und den schutzwürdigen Interessen der Mitarbeiter ergab, dass wegen des hier betriebenen reinen Monitoring der Eingriff in die Persönlichkeitsrechte der Mitarbeiter als nur gering einzustufen war und damit das berechtigte Überwachungsinteresse überwog.
An dieser Stelle möchte ich anmerken, dass eine Videoüberwachung im Beschäftigungsverhältnis, sofern sie nicht auf eine Rechtsgrundlage gestützt werden kann, nach § 4 Abs. 1 BDSG (Verbot mit Erlaubnisvorbehalt) unzulässig ist. Eine etwaige arbeitgeberseitig eingeholte Einwilligung des Beschäftigten ist irrelevant, da es im Beschäftigungsverhältnis in der Regel an der Freiwilligkeitsvoraussetzung des § 4 a Absatz 1 Satz 1 BDSG mangelt. Eine freiwillige Information des Unternehmens gegenüber seinen Beschäftigten über Art, Zweck und Umfang einer durchgeführten Videoüberwachung ist im Sinne des Transparenzgedankens, der das BDSG durchzieht, ebenso zu begrüßen wie Betriebsvereinbarungen zur Videoüberwachung. Allerdings existiert in der Fleisch verarbeitenden Industrie oft kein Betriebsrat.

Überwachung der Verladung und der Lkw-Stellplätze zulässig

Die Schlachtbetriebe machten darüber hinaus ein Interesse an einer Videoüberwachung der Endverladung ihrer Fleischprodukte auf Lkw geltend, da es trotz Verplombung immer wieder zu Ladungsverlusten kommen soll. Ziel der Videoüberwachung ist daher die Sicherung von Beweisen im Falle eines solchen Ladungsverlusts. Eine solche Videodokumentation ist im Fall der Produktversendung unter Nutzung von Speditionen oder bei Abholung der Produkte durch Unternehmen datenschutzrechtlich nicht zu beanstanden. Werden die Produkte aber durch unternehmenseigene Lkw zum Kunden geliefert, ist die Überwachung auf eine Standbilddarstellung zu reduzieren.
Meine Prüfungen erstreckten sich auch auf das Betriebsgelände, da unter anderem die Lkw-Stellplätze aufgrund des häufig auftretenden Dieseldiebstahls mit Kameras überwacht

werden. Hier forderte ich eine Videoüberwachung als reines Monitoring ohne Aufzeichnung der Bilddaten, wobei personell und organisatorisch die Möglichkeit einer Intervention sicherzustellen war. Dem trugen die geprüften Betriebe dadurch Rechnung, dass die Videobilder auf einem Monitor im Pförtnerbüro am Eingang des Geländes auflaufen. So besteht im Deliktsfall auch aufgrund der steten personellen Präsenz die Möglichkeit zur Intervention.

Im Rahmen der Beratung teilte ich einem Unternehmen mit, dass die auf eigenem Grundstück außerhalb der Werkseinfriedung liegenden Brunnen für die Wasserversorgung im Rahmen der Lebensmittelsicherheit überwacht werden dürfen. Ergänzend empfahl ich, das nicht eingefriedete Gelände mit Hinweisschildern zur Eigentumsangabe zu versehen.

Die Wichtigkeit einer klaren Kennzeichnung der Besitz- und Eigentumsverhältnisse zeigte sich auch bei einer anderen Prüfung. Hier ergab die Vor-Ort-Kontrolle, dass die Kameras aufgrund ihrer guten Zoomfunktion auch das vor der Einzäunung liegende Gelände erfassen konnten. Dieser Bereich wurde nach Mitteilung der Unternehmensleitung jedoch teilweise von Aktivisten einer Bürgerinitiative für ihre Demonstrationen gegen diesen Schlachtbetrieb genutzt. Auf Nachfrage erfuhr ich, dass es sich bei den dahinterliegenden Bereichen überwiegend auch um betriebseigene Flächen handelt, die für geplante Erweiterungen bereits seitens des Unternehmens aufgekauft worden waren. Da für Außenstehende jedoch nicht erkennbar ist, dass auch Flächen vor dem eingezäunten Bereich zum Unternehmen gehören, empfahl ich, dies durch entsprechende Hinweisschilder kenntlich zu machen. Im Übrigen beanstandete ich die Videoüberwachung nicht. Allerdings wies ich in allen überprüften Fällen klarstellend darauf hin, dass bei der Anbringung von Kameras zur Beobachtung des Zauns und zur Verhinderung unbefugten Betretens (Wahrnehmung des Hausrechts) zu beachten ist, dass die Beobachtungsbefugnis des Hausrechtsinhabers und Grundstückseigentümers grundsätzlich an der Grundstücksgrenze (vgl. BGH NJW 1995, Seite 1954,1955) endet. Im Einzelfall darf jedoch im geringen Umfang hierüber hinausgegangen werden, wenn ein Toleranzbereich eingehalten wird, der zur effektiven Überwachung zum Schutz des Eigentums und der Zugangskontrolle erforderlich ist (vgl. Urteil des Amtsgerichts Berlin-Mitte vom 18. Dezember 2003, Az.: 16 C 427/02).

Zahlreich und hochauflösend

Bei beiden Schlachthöfen waren die Videokameras so zahlreich und von so hochauflösender Technik, dass stets eine Vorabkontrolle nach § 4 d Abs. 5 BDSG durchzuführen war. Da die Zuständigkeit für eine Vorabkontrolle nach § 4 d Abs. 5 BDSG beim betrieblichen Datenschutzbeauftragten liegt (§ 4 d Abs. 6 BDSG), bestand bereits aufgrund dieses Umstands eine Bestellpflicht gem. § 4 f Abs. 1 Satz 6 BDSG.

In einem Fall erklärte das Unternehmen, dass es die gewonnenen Erkenntnisse aus diesem Kontrollverfahren so auch auf die weiteren vier Betriebe des Unternehmens in Deutschland übertragen werde.

Weitere Informationen:

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ unter www.lfd.niedersachsen.de > Themen > Videoüberwachung > Videoüberwachung durch private Stellen und Unternehmen

Effektiver Datenschutz im Kaufhaus: Aus 120 Kameras werden 60

Ausgelöst durch einen Zeitungsbericht über die Videoüberwachung in der Filiale eines großen Textilkaufhauses führte ich im Berichtszeitraum eine umfangreiche Kontrolle durch, die weitreichende Veränderungen nach sich zog. Der Prüfung und rechtlichen Würdigung der zunächst erbetenen Unterlagen schloss sich eine Vor-Ort-Kontrolle im Geschäft an.

Das weltweit agierende Unternehmen hatte zu diesem Zeitpunkt bereits erkannt, dass es professioneller Unterstützung bedurfte, und mit der Wahrnehmung der Aufgabe der betrieblichen Datenschutzbeauftragten eine große, auf Datenschutz spezialisierte Anwaltskanzlei beauftragt. Die geprüfte Videoüberwachung mit über 120 Kameras entsprach zu diesem Zeitpunkt auch nicht den Anforderungen des Bundesdatenschutzgesetzes (BDSG).
Formalrechtlich beanstandete ich, dass das Hinweisschild nicht den Anforderungen des § 6 b Abs. 2 BDSG genügte, da die Angabe der verantwortlichen Stelle fehlte und es so angebracht war, dass es nicht vor Betreten des überwachten Bereichs problemlos wahrnehmbar war. Zudem widersprach die Speicherfrist von mehr als 72 Stunden dem Gebot der unverzüglichen Löschung aus § 6 b Abs. 5 BDSG. Auch die Kameraüberwachung war in großen Teilen unzulässig. Zudem wurde vielfach im Übermaß überwacht, was dem Grundsatz der Datensparsamkeit aus § 3 a BDSG widersprach.
In der Folge reduzierte die Firma unter anderem die über den Kassentresen angebrachten Videokameras um die Hälfte. Bei den verbliebenen Kassenkameras wurde der Erfassungsbereich so eingeschränkt, dass die Kassenarbeitsplätze hinter dem Tresen und die PIN-Eingabegeräte nicht mehr überwacht werden. An den Kundeneingängen befanden sich Monitore, die jedoch nicht nur die das Geschäft betretenden Kunden zeigten, sondern auch den Straßenbereich dahinter. Auch hier wurde der Erfassungsbereich der Kamera eingeschränkt.

Mitarbeiterüberwachung grundsätzlich unzulässig

Bei der Prüfung zeigte sich als besondere Problematik die Überwachung des Personals. Diverse Kameras erfassten Bereiche, die (nahezu) ausschließlich vom Personal genutzt wurden. Diese lagen insbesondere jenseits der Verkaufsräume im Untergeschoss sowie im Personalverwaltungsbereich darüber. Des Weiteren überwachten Kameras Mitarbeiter-Treppenhäuser, Fahrstühle für Mitarbeiter sowie ausschließlich von Mitarbeitern genutzte Lastenaufzüge. Hier galt es zwischen dem teilweise durchaus berechtigten Interesse des Unternehmens und den entgegenstehenden schutzwürdigen Interessen der betroffenen Mitarbeiter abzuwägen. Dabei wurden auch die Eingriffsintensität und der Transparenzgedanke thematisiert. Aufgrund meines Hinweises auf die Rechtsprechung des Bundesarbeitsgerichts baute die Firma schließlich alle entsprechenden Kameras ab.

Die Fundstelle des Bundesarbeitsgerichtsbeschlusses finden Sie in meiner Orientierungshilfe „Videoüberwachung durch nicht- öffentliche Stellen" unter www.lfd.niedersachsen.de > Themen> Videoüberwachung > Videoüberwachung durch private Stellen und Unternehmen.

Eine unzulässige Arbeits- und Leistungskontrolle mit der Folge eines Verstoßes gegen § 32 Abs. 1 S. 2 BDSG ist nun nicht mehr zu befürchten.

Nicht nur deaktiviert, sondern abgebaut

Wegen der hier betroffenen Mitarbeiter hat sich das Unternehmen dazu entschlossen, nicht nur die rechtlich zu fordernde Deaktivierung der datenschutzwidrigen Kameras zu veranlassen. Sie hat die Kameras vielmehr sogar entfernen lassen, was besonders begrüßenswert ist.
Bei dem im Bereich der Kunden-Treppenhäuser für die Videoüberwachung genannten maßgeblichen Zweck der Überwachung von Fluchtwegen reicht ein reines Beobachten (Live-Monitoring) aus, weshalb die regelmäßig eingriffsintensivere zusätzliche Aufzeichnung nicht erforderlich und somit datenschutzrechtlich unzulässig ist. Auch diese Vorgaben akzeptierte das Unternehmen, so dass die Überwachung der Kunden-Treppenhäuser nun rechtskonform als reines Live-Monitoring ohne Aufzeichnung erfolgt. Die Überwachung der Kunden-Fahrstühle musste ich ebenfalls beanstanden, da diese einen weitreichenden Eingriff in die Persönlichkeitsrechte der Betroffenen darstellt. Die fehlende Ausweichmöglichkeit und der daraus resultierende ständige Überwachungsdruck begründen hier ein Überwiegen der schutzwürdigen Interessen der Betroffenen und damit letztlich die Unzulässigkeit der Videoüberwachung.
Grundsätzlich nicht beanstandet wurde die Videoüberwachung in den Verkaufsbereichen mit sogenannten Dome-Kameras (Monitoring und Aufzeichnung). Allerdings musste die Firma durch technische Maßnahmen (zum Beispiel Teilverpixelungen) sicherstellen, dass über die Zoomfunktion keine Mitarbeiterüberwachung ermöglicht wird. Die Überwachung der Rolltreppen im Monitoringmodus im Kaufhaus aus Gründen der Verkehrssicherungspflicht beanstandete ich ebenfalls nicht.
An der Umsetzung der datenschutzrechtlichen Anforderungen, die zu einer Reduzierung auf rund 60 Kameras führte, waren die betrieblichen Datenschutzbeauftragten im Rahmen eines Maßnahmenplanes maßgeblich beteiligt.

Neues Konzept auf alle Filialen übertragen

Nach datenschutzkonformer Umsetzung der Videoüberwachung kündigte das Unternehmen an, das für das niedersächsische Geschäft erarbeitete Konzept der eingeschränkten und auf das Wesentliche beschränkten Videoüberwachung so auch auf alle weiteren deutschen Filialen zu übertragen. Neue Filialen würden gleich nach dem neuen Datenschutzkonzept gestaltet. Dies wurde auch den örtlichen Betriebsräten mitgeteilt.
Ich wies das Unternehmen während des Verfahrens darauf hin, dass die im Rahmen der konstruktiven Zusammenarbeit gefundenen datenschutzkonformen Regelungen zur Videoüberwachung nicht durch abweichende betriebliche Vereinbarungen unterlaufen werden dürfen.

Videoüberwachung in Einkaufspassage: Elf Kameras zu viel

Einer Eingabe folgend überprüfte ich die Videoüberwachung in einer Einkaufspassage, über die zahlreiche Einzelhandelsgeschäfte und gastronomische Betriebe zugänglich sind. Die Passage wird von einer Betreibergesellschaft bewirtschaftet, die jedoch dort keinen eigenen Einzelhandelsbetrieb unterhält, und ist von sehr vielen Zugängen aus erreichbar, unter anderem auch von mehrgeschossigen Kaufhäusern. Sie muss sowohl von Kunden der anliegenden Geschäfte, als auch von den Nutzern öffentlicher Verkehrsmittel durchquert werden, ohne dass diese eine Möglichkeit haben, die Passage und damit die Videoüberwachung zu umgehen.

Die Videoüberwachung erfasste nicht nur den gesamten Passagenbereich bis zu den Eingängen der angrenzenden Geschäfte und Gastronomiebetriebe, sondern auch Treppenaufgänge und Rolltreppen. Sie erfolgte rund um die Uhr mit 25 Kameras. Die Videodaten wurden auf drei Monitoren in einem gesonderten Kontrollraum von Sicherheitspersonal der Betreibergesellschaft in Echtzeit beobachtet und zudem bis zu 48 Stunden gespeichert. Eine den Anforderungen des § 6 b Abs.2 Bundesdatenschutzgesetz (BDSG) nicht genügende Kennzeichnung führte dazu, dass die Überwachung für Betroffene nicht ausreichend erkennbar war.
Bei der Passage handelt es sich um öffentlich zugänglichen Raum, sodass die Zulässigkeit der Videoüberwachung nach Maßgabe des § 6 b Abs. 1 Nr. 2 und 3 und Abs. 3 BDSG zu prüfen war. Eine Videoüberwachung muss demnach zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke geeignet und erforderlich sein, und es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Auch

muss die Videoüberwachung mit dem Gebot der Datenvermeidung und Datensparsamkeit, das sich aus § 3 a BDSG ergibt, im Einklang stehen.
Die Videoüberwachung sollte dem Objektschutz, der Sicherstellung der Hausordnung und der Beweissicherung bei Straftaten und Vandalismus dienen. Meine Prüfung ergab jedoch, dass einige der Kameras ausschließlich zur Unterstützung der Polizei verwendet wurden. Diese hatte gerne auf die Aufzeichnungen zurückgegriffen, um gegen Straftäter zu ermitteln, die anderen Passanten in der Passage oder in deren näherem Umfeld Schaden zugefügt hatten. In diesen Fällen wurden die gespeicherten Videoaufnahmen folglich nicht, wie vom Gesetz verlangt, für die Wahrnehmung eigener Interessen des Passagenbetreibers verwendet. Daher waren einige Kameras datenschutzrechtlich unzulässig und wurden vom Passagenbetreiber nach meiner datenschutzrechtlichen Beratung deaktiviert.

Abstrakte Gefahrenvorsorge reicht nicht als Begründung

Auf meinen weiteren Hinweis, dass die Überwachung nicht mit dem Ziel einer abstrakten Gefahrenvorsorge begründet werden könne, sondern durch dokumentierte Ereignisse aus der Vergangenheit nachzuweisen sei, reduzierte die Betreibergesellschaft die Videoüberwachung um weitere Kameras, die nach den von ihr vorgelegten Unterlagen diesen Kriterien nicht genügten. Letztlich verblieben noch 14 Kameras, die grundsätzlich zur Hausrechtsausübung oder zur Wahrnehmung berechtigter Interessen der Betreibergesellschaft betrieben werden durften. Sie wurden aufgrund meiner Beratung jedoch teilweise neu ausgerichtet und auf kritische Bereiche fokussiert.
Außerdem vereinbarte ich im Rahmen meiner Vor-Ort-Kontrolle mit den Verantwortlichen der Betreibergesellschaft, dass an allen Zugangsbereichen der Passage an gut sichtbarer Stelle und Höhe Hinweisbeschilderungen mit Bezeichnung der verantwortlichen Stelle, so wie es § 6 b Abs.2 BDSG verlangt, angebracht werden.

Aufzeichnung nur, wenn nötig

Darüber hinaus konnten die Verantwortlichen der Betreibergesellschaft, denen vor allem eine wirksame Ausübung ihres Hausrechtes mit Hilfe der Videokameras ein wichtiges Anliegen ist, davon überzeugt werden, dass die Videoüberwachung insbesondere zur Wahrnehmung dieses Zwecks nur dann effektiv eingesetzt werden kann, wenn dies durch das Beobachten von Monitoren („Monitoring“) in Echtzeit geschieht, weil nur hierdurch der beauftragte Sicherheitsdienst in der Lage ist, gezielt und angemessen auf Hausrechtsverstöße und zum Nachteil der Betreibergesellschaft begangene Sachbeschädigungen zu reagieren. Künftig werden daher die verbliebenen 14 Kameras durchgehend nur noch im Monitoringmodus betrieben. Eine darüber hinausgehende Aufzeichnung der Videodaten wird von den Mitarbeitern des Sicherheitsdienstes nur dann initiiert, wenn ein Ereignis eintritt, das die Sicherung der Aufnahmen zu Beweiszwecken erforderlich macht.
Diese Ausgestaltung der Videoüberwachung findet vor allem deshalb meine ausdrückliche Billigung, weil damit dem datenschutzrechtlichen Grundsatz der Datenvermeidung und Datensparsamkeit in vorbildlicher Weise entsprochen wird.

Weitere Informationen:

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ unter www.lfd.niedersachsen.de > Themen > Videoüberwachung > Videoüberwachung durch private Stellen und Unternehmen

Webcams in touristischen Gebieten: Blick in den Strandkorb

Fernweh und keinen Reiseprospekt zur Hand? Schauen Sie sich doch mal Live-Bilder oder -Videos vom Reiseziel im Internet an! Wie mag es wohl an meinem Traum-Urlaubsort aussehen? Sind die Strandkörbe voll? Liegt genug Schnee auf der Piste? Diesen Informationsbedarf versuchen viele Tourismusverbände, Hotelbetreiber und Anbieter von Ferien- und Freizeitattraktionen mit dem Einsatz von Webcams zu decken.

Webcams ermöglichen es, Live-Aufnahmen ins Internet einzustellen und damit einer unbestimmten Zahl von Personen weltweit zugänglich zu machen. Damit kann man das Interesse vieler Menschen auf ein touristisches Ziel richten, aber man kann auch vieles falsch machen. Problematisch beim Einstellen der Video-Daten in das Internet ist nämlich, dass Persönlichkeitsrechtsverletzungen bei einer Live-Übertragung nicht mehr rückgängig gemacht werden können. Der Einsatz von Webcams ist daher nur dann datenschutzrechtlich unbedenklich, wenn auf den aufgenommenen Bildern keine Personen oder personenbeziehbare Daten wie zum Beispiel Kfz-Kennzeichen erkennbar sind.

Die Zahl der eingesetzten Webcams nimmt ebenso stetig zu, wie die Zahl der Menschen, die sich dadurch in Echtzeit in ihrer Freizeit beobachtet und in ihrem Recht am eigenen Bild verletzt fühlen. Das zeigt jedenfalls eine steigende Zahl von Eingaben. Dies habe ich zum Anlass genommen und das World Wide Web stichprobenhaft nach Webcams in touristischen Gebieten von der Weser bis zur Elbe, vom Harz bis ans Meer durchsucht. Dabei konnte ich den Leuten beim Spaziergang am Strand zusehen, beim Essen, beim Sonnen, beim Klönen auf einer Parkbank und einiges mehr. Sogar der Blick in den Strandkorb war möglich.

Nur Übersichtsaufnahmen, keine Details!

Sobald Personen erkennbar waren, habe ich mich mit den Betreibern der Webcams in Verbindung gesetzt und auf die Unzulässigkeit der Verbreitung der Aufnahmen aufmerksam gemacht. Denn auch hier überwiegt das Interesse der Betroffenen daran, sich unbeobachtet in der Öffentlichkeit bewegen zu können, gegenüber dem Interesse der Kamerabetreiber, den Urlaubsort in möglichst positiven und anpreisenden Bildern zu zeigen. Auf § 6 b Abs.1 Nr. 3 und Abs. 3 Bundesdatenschutzgesetz (BDSG) als einzige denkbare datenschutzrechtliche Erlaubnisvorschrift kann also schon aus diesen Gründen nicht zurückgegriffen werden.

Die Betreiber der Webcams mochten regelmäßig allerdings nicht ganz auf Fotos und Videos verzichten und griffen meine Vorschläge für einen datenschutzkonformen Betrieb daher zumeist dankbar auf. Oft reichte es hierfür aus, den Erfassungswinkel der Kameras so zu verändern, dass nicht mehr auf Bereiche in der Nähe fokussiert wurde, sondern die Aufnahmen eher eine Übersichtsfunktion erfüllten. Und so konnte auch ich dann mit der beruhigenden Gewissheit eines datenschutzgerechten Webcam-Einsatzes die touristisch reizvollen Regionen Niedersachsens via Internet betrachten.

Weitere Informationen:

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ unter www.lfd.niedersachsen.de > Themen > Videoüberwachung > Videoüberwachung durch private Stellen und Unternehmen

Wildwuchs bei Wildkameras: Videoüberwachung im Wald nur selten zulässig

Nicht alles, was an Bäumen hängt, wächst auch dort. Immer mehr Wildkameras werden am Gehölz befestigt und beobachten den Wald und alles, was sich darin bewegt.

Grundsätzlich ist der Wald frei für alle zugänglich, sofern es keine besonderen rechtlichen Einschränkungen gibt. Da der Wald eigentlich eine der letzten technikfreien Zonen sein sollte, sind viele Waldbesucher, die dort Ruhe und Entspannung suchen, verständlicherweise genervt, wenn sie selbst dort nicht vor Videotechnik in Form einer Wildkamera verschont sind. Einerseits ist der Tritt in die Fotofalle nicht vorhersehbar, andererseits weiß man meist nicht, wer einen per Bildaufnahme festhält. Denn zumeist fehlt der erforderliche Hinweis nach § 6 b Abs. 2 Bundesdatenschutzgesetz (BDSG), dass eine Beobachtung erfolgt und wer für diese verantwortlich ist.
Gravierender als die fehlende Hinweisbeschilderung ist allerdings die fehlende Rechtsgrundlage für den Einsatz einer Wildkamera im Wald. Selbst wenn eine Videoüberwachung im Einzelfall für die Wahrnehmung berechtigter Zwecke erforderlich sein mag (§ 6 b Abs. 1 Nr. 3 BDSG), kann man davon ausgehen, dass die schutzwürdigen Interessen der Betroffenen vor allem dort überwiegen, wo die Menschen im Wald zu Recht einen unbeobachteten Aufenthalt in der freien Natur erwarten dürfen. Das gilt insbesondere für Waldwege, aber auch für Lichtungen und sonstige Bereiche des Waldes, die ohne weiteres zu Fuß erreicht werden können. Eine Videoüberwachung in den öffentlich zugänglichen Bereichen des Waldes ist daher grundsätzlich unzulässig.
Eine Ausnahme kann die Beobachtung seltener oder neu angesiedelter Tierarten im Rahmen eines Artenschutzprogramms darstellen. In diesem Fall sollte die Tierbeobachtung möglichst im Rahmen einer Beauftragung durch eine öffentliche Stelle erfolgen. So werden in Niedersachsen bereits zahlreiche Kameras zur Entwicklung der Wolfspopulation und zur Dokumentation seiner Ausbreitung sowie zur Begleitung der Wiederansiedlung von Luchsen eingesetzt. Ist der Betrieb einer Wildkamera datenschutzrechtlich zulässig, sind neben der Hinweispflicht aber auch weitere Vorschriften zu beachten. So gilt die Pflicht, ein Verfahrensverzeichnis vorzuhalten (§ 4 e BDSG) und dieses auf Antrag jedermann zugänglich zu machen (§ 4 g Abs. 2 BDSG). Zudem unterliegt der Betrieb einer Wildkamera im öffentlich zugänglichen Raum der Pflicht zur Meldung an die zuständige Aufsichtsbehörde.

Darf beobachtet werden: Canis lupus (Quelle: Wikipedia, Martin Mecnarowski)

Fotofallen nicht datenschutzrelevant

Nicht den Vorschriften des BDSG unterliegen Wildkameras, die außerhalb der für jedermann zugänglichen Bereiche des Waldes angebracht sind, wie zum Beispiel in Schonungen und jagdlichen Einrichtungen. Auch sogenannte Fotofallen, die nur Einzelaufnahmen fertigen, sind nicht datenschutzrelevant, da bei ihnen nicht der Tatbestand der „Beobachtung“ im Sinne des § 6 b Abs.1 BDSG vorliegt. Allerdings können Betroffene gegen solche Fotofallen wegen eines möglichen Verstoßes gegen das Kunsturhebergesetz zivilrechtlich vorgehen.

Weitere Informationen:

www.lfd.niedersachsen.de > Themen > Videoüberwachung > Videoüberwachung durch private Stellen und Unternehmen > Orientierungshilfe Videoüberwachung mit Wildkameras.pdf

Videoüberwachung an Schulen: Meistens unzulässig

Die vielen Anfragen von Schulen und Schulträgern zum Einsatz von Videoüberwachungstechnik und auch zahlreiche Beschwerden der von der Überwachung betroffenen Personen veranlassten mich Ende 2014, meine Orientierungshilfe zur Videoüberwachung an öffentlichen Schulen im Land Niedersachsen zu überarbeiten und neu zu fassen. Sie ist auf meiner Homepage nachzulesen.

Zusammenfassend ist festzustellen, dass eine Videoüberwachung, die immer tief in das Recht auf informationelle Selbstbestimmung der beobachteten und aufgezeichneten Person eingreift, nur unter strikter Beachtung des Verhältnismäßigkeitsgrundsatzes zulässig ist. Des Weiteren ist von entscheidender Bedeutung, ob die Videoüberwachung

- während oder
- außerhalb der Schulzeiten
- in einem öffentlich zugänglichen Bereich oder
- in einem nicht öffentlich zugänglichen Bereich

erfolgen soll.

Bis auf wenige, besonders zu begründende Einzelfälle ist eine Videoüberwachung während der Schulzeiten nicht zulässig, unabhängig, ob sie in öffentlich zugänglichen oder öffentlich nicht zugänglichen Räumen durchgeführt wird.
Aber auch außerhalb der Schulzeiten muss die Videoüberwachung erforderlich sein, das heißt, es dürfen keine anderen zumutbaren Möglichkeiten wie zum Beispiel verstärkte Kontrollen durch Personal, Einzäunung des Geländes, Bewegungsmelder mit Scheinwerfern und Alarmanlagen bestehen, um den beabsichtigten Zweck der Videoüberwachung zu erreichen. Zudem muss sie verhältnismäßig sein, es müssen also die Interessen der Schule gegen die schutzwürdigen Interessen der von der Überwachung Betroffenen abgewogen werden.
Folglich ist eine Videoüberwachung an Schulen immer anhand des Einzelfalles zu überprüfen. Sie ist „als letztes Mittel“ nur dann zulässig, wenn andere Maßnahmen nicht zumutbar sind oder keinen Erfolg versprechen.

Weitere Informationen:

Orientierungshilfe Videoüberwachung an öffentlichen Schulen unter
www.lfd.niedersachsen.de > Themen > Schulen

Videoüberwachte Gerichtsgebäude: Hinweisschilder oft nicht wahrnehmbar

Einen Schwerpunkt meiner beratenden Tätigkeit im Berichtszeitraum nahm die Videoüberwachung durch Behörden und andere öffentliche Stellen ein. Hierbei habe ich in acht Fällen die Videoüberwachung an und in Gerichtsgebäuden geprüft und im Einvernehmen mit den jeweils verantwortlichen Stellen Veränderungen im Sinne des § 25 a Niedersächsisches Datenschutzgesetz (NDSG) bewirkt.

Ein wesentliches Ergebnis der Kontrollen war, dass es bei einigen Videoüberwachungsmaßnahmen an der Erforderlichkeit und Geeignetheit fehlte. So gab es Fälle, in denen eine Einlasskontrolle zum Schutz von Personen und Sachen, die der beobachtenden Stelle angehören oder zu ihnen gehören, als Zweck der Überwachung genannt wurde. Durchgeführt wurde jedoch lediglich eine Aufzeichnung der Videobilder, ohne dass es zu einer „Inaugenscheinnahme" der Personen oder mitgeführten Sachen vor dem Betreten des Gebäudes kam.

Aufzeichnung nicht erforderlich

Ich beriet die verantwortlichen Stellen dahingehend, dass eine Einlasskontrolle zu dem genannten Zweck nur erforderlich und geeignet sein könne, wenn die Eingangstüren zunächst verschlossen sind und Einlass begehrende Personen in einer Echtzeitbeobachtung auf einem Monitor in Augenschein genommen werden, bevor die Tür geöffnet wird. Eine Aufzeichnung dieser Daten sei im Sinne einer präventiven Maßnahme weder erforderlich noch geeignet. In diesem Punkt waren alle beteiligten Personen einsichtig, und die Einlasskontrollen wurden gesetzeskonform angepasst.
Weitere Mängel stellte ich im Bereich der Erkennbarkeit der Überwachung und der Angabe der verantwortlichen Stelle durch Hinweisschilder fest. In mehreren Fällen war die Beschilderung in einer Flut von weiteren Hinweisschildern nicht eindeutig erkennbar und auch erst wahrnehmbar, wenn der überwachte Bereich bereits betreten worden war. Auch hier führten die Gespräche zu einer Änderung in der Beschilderung, die nun rechtzeitig und eindeutig wahrnehmbar ist. Außerdem unterbreitete ich Vorschläge, wie beispielsweise auf eine Videoüberwachung hingewiesen werden kann, die nur temporär durchgeführt wird.

Seminar im Datenschutzinstitut

Besonders positiv möchte ich die frühzeitige Beteiligung an dem Neubau eines so genannten Fachgerichtszentrums in Hannover hervorheben, bei dem ich vor dem eigentlichen „ersten Spatenstich“ beratend tätig werden konnte. Hier gelang es, die Videoüberwachungsanlagen bereits vor dem Kauf datenschutzrechtlich zu beurteilen und die Erstellung der nötigen Dokumente zu veranlassen:

- Vorabkontrolle gemäß § 7 Abs. 3 NDSG,
- Verfahrensbeschreibung nach § 8 NDSG,
- Dienstvereinbarung zum Ausschluss einer Verhaltens- und Leistungskontrolle der Mitarbeiter des Fachgerichtszentrums.

Ich habe mich kurzfristig entschlossen, in meinem Datenschutzinstitut ein Seminar mit Workshopinhalten zum Thema „Videoüberwachung durch die öffentliche Hand“ anzubieten, um die erlangten Erkenntnisse vielen Interessierten zugänglich zu machen.

Weitere Informationen:

www.lfd.niedersachsen.de > Themen > Videoüberwachung > Videoüberwachung durch öffentliche Stellen

9. Europa und internationaler Datenverkehr

Europäische Datenschutzreform: Ein Ende ist nicht in Sicht

Die EU-Kommission leitete im Jahre 2012 mit Vorlage eines Entwurfs für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr den lang erwarteten Reformprozess des Europäischen Datenschutzrechts ein. Die Entwürfe enthalten wesentliche Änderungen zum aktuell geltenden Datenschutzrecht und begegneten teils starker Kritik. Insbesondere wird befürchtet, dass die hohen Datenschutzstandards in Deutschland abgesenkt werden könnten.

Im März 2014 beschloss das EU-Parlament ein Verhandlungsdokument, das auf dem Vorschlag der EU-Kommission für eine Datenschutz-Grundverordnung basiert, aber einige Änderungen enthält:

- Vor allem unterstützt das EU-Parlament den Ansatz der EU-Kommission zur vollen Harmonisierung des Datenschutzrechts; das Rechtsinstrument der Verordnung und der umfassende Anwendungsbereich wurden vom Parlament folglich übernommen.
- Die im Entwurf der Kommission eingeräumten und kritisierten Kompetenzausweitungen der Kommission hat das Parlament in seinem Entwurf stark reduziert.
- Den ebenfalls umstrittenen Grundsatz des „One-Stop-Shop“ (bei in mehreren Mitgliedstaaten tätigen Unternehmen ist nur die an der Hauptniederlassung des Unternehmens sitzende Aufsichtsbehörde zuständig) hat das Parlament insofern geändert, als dass künftig nur die Aufsichtsbehörde am Hauptsitz des Unternehmens federführend zuständig sein soll und nur nach Konsultation der anderen betroffenen Aufsichtsbehörden tätig werden darf.
- Die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten knüpft das Parlament anders als die Kommission nicht an die Anzahl der Mitarbeiter eines Unternehmens, sondern an die Anzahl der von der Daten-

verarbeitung betroffenen Personen innerhalb eines Zeitraums von 12 Monaten: Bei mindestens 5.000 betroffenen Personen besteht eine Pflicht zur Bestellung eines Datenschutzbeauftragten.

- Vor dem Hintergrund der bekannt gewordenen massenhaften Ausspähungen von Daten durch Geheimdienste hat das Parlament in seinem Entwurf zum Bereich internationaler Datenverkehr eine Regelung ergänzt, wonach Anweisungen und Urteile, die Unternehmen zur Herausgabe von personenbezogenen Daten verpflichten, aber gegen EU-Datenschutzrecht verstoßen, nur nach Zustimmung der Aufsichtsbehörden vollstreckt werden dürfen.
- Zu verschiedenen Regelungen des Kommissionsentwurfs hat das Parlament Konkretisierungen und Verschärfungen erstellt, etwa zu Fragen der Einwilligung der betroffenen Person, zum Verbandsklagerecht, zur Pflicht zur Datenlöschung, zum Marktortprinzip.
- Der Parlamentsentwurf entschärft nur einige auch von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder geäußerten Kritikpunkte zum Kommissionsentwurf, vermag aber selbst nicht vollumfänglich die im Verfahren von verschiedener Seite geäußerten Bedenken insbesondere hinsichtlich der befürchteten Absenkung des in Deutschland herrschenden hohen Datenschutzniveaus auszuräumen.

Verhandlungen im Rat der EU

Auch der Ministerrat der EU beschäftigt sich nun wie nach dem europäischen Gesetzgebungsverfahren vorgesehen mit der Datenschutz-Grundverordnung. Hier verhandeln die Vertreter der Mitgliedstaaten in der Ratsarbeitsgruppe Datenschutz und Informati-

onsaustausch über eine Annahme der vorgelegten Entwürfe oder deren Änderung. Zu den besonders umstrittenen Bereichen gehören auch hier

- der Anwendungsbereich der Grundverordnung auch auf öffentliche Stellen,
- der Grundsatz des „One-Stop-Shop“,
- die Bestellungspflicht hinsichtlich betrieblicher Datenschutzbeauftragter,
- die Problematiken des internationalen Datenverkehrs, der Auftragsdatenverarbeitung und der Betroffenenrechte.

Hier wurden und werden aus den Mitgliedstaaten verschiedene Vorschläge für Änderungen und auch Ergänzungen unterbreitet. Die Bundesregierung hat zum Beispiel zusätzlich einen neuen Punkt eingebracht und vorgeschlagen, dass die Aufsichtsbehörden die Rechtmäßigkeit oder Rechtswidrigkeit von bestimmten Datenverarbeitungsverfahren auf Antrag des datenverarbeitenden Unternehmens oder der betroffenen Person feststellen.

Entschließung der DSB-Konferenz

Mit ihrer Entschließung vom März 2014 „zur Struktur der künftigen Datenschutzaufsicht in Europa“ meldete sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erneut im Reformprozess zu Wort. Die Entschließung befasst sich mit Fragen zur Zuständigkeit und zu den Aufgaben der Aufsichtsbehörden. Besonderer Wert wurde auf die Feststellung gelegt, dass die Aufsichtsbehörde eines Mitgliedstaates weiterhin die Befugnis zur Aufsicht über alle Datenverarbeitungen, die Personen ihres Hoheitsgebietes betreffen, behalten muss. Daneben wurde darauf hingewiesen, dass kein Bedarf an der Einführung von Verfahren zur Feststellung von EU-weit gültigen Compliance-Entscheidungen besteht, bei welchen die datenschutzrechtliche Verantwortung von den Unternehmen auf die Aufsichtsbehörden verlagert würde.
Weitere Entwicklungen in den Verhandlungen sind nicht auszuschließen. Es bleibt abzuwarten, ob ein neues EU-Datenschutzrecht den hohen Erwartungen, die mit der Reform verbunden waren, gerecht wird.

Internationaler Datenverkehr und Geheimdiensttätigkeit: Sind die USA (noch) ein „sicherer Hafen“?

Mit den Enthüllungen des ehemaligen Geheimdienstmitarbeiters Edward Snowden über die Praxis der massenhaften Ausspähung von personenbezogenen Daten durch den US-amerikanischen Geheimdienst NSA änderte sich die Betrachtung des internationalen Datenverkehrs grundlegend. Eine Datenübermittlung aus Europa zu Stellen in einem Drittland wie die USA ist nach europäischem Datenschutzrecht nur zulässig, wenn das datenempfangende Unternehmen ausreichende Datenschutzstandards garantiert, zum Beispiel durch die Verwendung der EU-Standardvertragsklauseln, von unternehmensinternen Datenschutzregelungen (Binding Corporate Rules) oder unter Bezugnahme auf das Safe-Harbor-Abkommen. Seit den Enthüllungen von Edward Snowden ist in Frage gestellt, ob solche Garantien noch gegeben werden können.

Wir wissen heute, dass US-amerikanische Geheimdienste und Geheimdienste anderer Länder massenhaft und anlasslos die Telekommunikation und das Internet global abhören und ausspähen. Der bekannteste Fall ist sicher das Abhören des Handys von Bundeskanzlerin Merkel. Die Überwachung erfolgt unerkannt oder auch unter der – durch staatliche Anweisung erzwungenen – Mitwirkung von Unternehmen. Eine Information an die betroffenen Personen erfolgt nicht. Dieser massive Zugriff Dritter auf personenbezogene Daten ohne Begründung und Überprüfbarkeit im Einzelfall bedeutet einen Verstoß gegen die europäischen Datenschutzprinzipien. Die Gewährleistung eines ausreichenden Datenschutzstandards bei Übermittlung von personenbezogenen Daten in einen fremden Rechtsraum ist daher mehr als zweifelhaft.

Reaktionen

In ihrer Pressemitteilung vom 24. Juli 2013 nahm die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstmalig Stellung zum Thema Geheimdienstausspähungen: Es bestehe eine hohe Wahrscheinlichkeit für die Verletzung von europäischen Datenschutzgrundsätzen, daher hätten die Aufsichtsbehörden für den Datenschutz die Befugnis, internationale Datenübermittlungen auszusetzen und keine neuen Genehmigungen hierfür zu erteilen. Mit Entschließung vom 5. September 2013 äußerte sich die Konferenz erneut zum Thema und forderte vor allem zu einer weiteren Aufklärung durch die Regierung auf und erinnerte eindringlich an die staatliche Pflicht zum Schutz der Grundrechte. Die Europäische Kommission entwickelte ein Strategiepapier zur Wiederherstellung des Vertrauens in die Datenübermittlungen in die USA, das derzeit noch mit den Partnern auf US-amerikanischer Seite verhandelt wird. Auf Bundesebene wurde der NSA-Untersuchungsausschuss eingerichtet. Das zunächst angedachte No-Spy-Abkommen kam aufgrund der Verweigerung der US-Seite nicht zustande.

Vorläufiges Fazit

Auch wenn die öffentliche Debatte über die massenhaften Ausspähungen durch fremde Geheimdienste zunächst lautstark geführt wurde, hat dies doch bisher offenbar nicht zu Änderungen in der Praxis geführt. Reformen der Regelungen zu geheimdienstlicher Überwachung wurden nicht beschlossen. Die Datenschutzaufsichtsbehörden sind befugt, Datenübermittlungen bei ausreichender Wahrscheinlichkeit der Verletzung von europäischen Datenschutzstandards zu verbieten. Dazu ist es bislang nicht gekommen. Letztlich bleibt es jedoch Aufgabe der Politik, die massenhafte Verletzung von Grundrechten zu verhindern, etwa durch internationale Abkommen mit einer wirksamen Kontrolle von Geheimdiensttätigkeiten.

Weitere Informationen:

www.lfd.niedersachsen.de
> Themen > Wirtschaft > Internationaler Datenverkehr

Safe Harbor – Ein sicherer Hafen?

Die US-Regierung behauptet, einen „sicheren Hafen" für personenbezogene Daten aus Europa zu gewährleisten, doch Zweifel sind berechtigt. Das Vertrauen der EU in die Einhaltung der vereinbarten Datenschutzstandards ist brüchig geworden.

Was ist Safe Harbor?

Hinter dem Schlagwort „Safe Harbor" verbirgt sich ein Abkommen zwischen der EU und den USA aus dem Jahr 2000 über die Gewährleistung datenschutzrechtlicher Kernprinzipien beim Umgang mit aus den EU-Mitgliedstaaten stammenden personenbezogenen Daten. Eine Übermittlung von Daten aus der EU in die USA ist nur zulässig, wenn bei den US-Unternehmen ein angemessenes datenschutzrechtliches Schutzniveau garantiert werden kann. Mit dem Beitritt zu diesem Abkommen und der Anerkennung der dort genannten datenschutzrechtlichen Grundsätze gewährleistet ein Unternehmen dieses angemessene Schutzniveau, und eine Übermittlung der Daten ist daher zulässig.

Kritik und Zweifel

Von Beginn an kritisierten Datenschützer, dass Unternehmen lediglich durch eine Selbstverpflichtung zur Einhaltung der Grundsätze des Abkommens als sicherer Hafen für personenbezogene Daten angesehen werden und eine Überprüfung der tatsächlichen Einhaltung der Datenschutzprinzipien nicht stattfindet. Bereits im Jahr 2010 verlangten die deutschen Datenschutzbehörden daher, dass die datenexportierenden Unternehmen in Deutschland sich nicht allein auf die Safe-Harbor-Zertifizierung einer Stelle in den USA verlassen dürfen; mindestens eine Prüfung der Gültigkeit der Zertifizierung und bezüglich der Einhaltung von Informationspflichten gegenüber den Betroffenen muss erfolgen. Der damalige Bundesbeauftragte für den Datenschutz forderte eine effektivere Kontrolle der Einhaltung der Safe-Harbor-Grundsätze.

Safe Harbor und die NSA

In ihrer Pressemitteilung vom 24. Juli 2013 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder angekündigt, die Aussetzung von Datenübermittlungen auf Grundlage des Safe-Harbor-Abkommens zu prüfen. Diese Prüfungen waren bis Ende 2014 noch nicht abgeschlossen. Eine solche Aussetzung ist möglich, wenn die hohe Wahrscheinlichkeit besteht, dass die Safe-Harbor-Grundsätze verletzt sind. Die Zulässigkeit der Übermittlung von personenbezogenen Daten von europäischen Unternehmen an Stellen in den USA ist daher fraglich.
Im November 2013 stellte die EU-Kommission Maßnahmen vor, die zur Wiederherstellung des Vertrauens in die Datenströme zwischen der EU und den USA erforderlich seien, darunter 13 Regelungen zur Verbesserung des Safe-Harbor-Abkommens. Die Verbesserungsvorschläge beschäftigen sich unter anderem mit Fragen der Transparenz, der Durchsetzung von Betroffenenrechten und den Datenzugriffen von US-Behörden. Über die Umsetzung dieser Vorschläge wird seitdem mit der US-Regierung verhandelt.

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

Mit der so genannten Art.-29-Gruppe hat die Europäische Union ein besonderes Gremium zur Betrachtung datenschutzrechtlicher Fragestellungen eingerichtet. In den Jahren 2013 und 2014 meldete sich die Gruppe zu vielen kontroversen Fragen lautstark zu Wort.

Die Einrichtung der Art.-29-Gruppe basiert auf Art. 29 der EU-Datenschutzrichtlinie 95/46/EG. Danach ist die Gruppe eine unabhängige Institution, welche die EU-Kommission in Datenschutzfragen berät, auf eine einheitliche Anwendung der allgemeinen Grundsätze der Datenschutzrichtlinie durch eine Zusammenarbeit der Aufsichtsbehörden hinwirkt und zu datenschutzrechtlichen Themen Stellung nimmt. Das Gremium besteht aus Vertretern der Aufsichtsbehörden, einem Vertreter des Europäischen Datenschutzbeauftragten sowie einem Vertreter der Kommission. Zu einzelnen Themenbereichen gibt es Unterarbeitsgruppen (Subgroups), so zum Beispiel die Technology Subgroup, die International Transfers Subgroup und die Financial Matters Subgroup. Über diese Unterarbeitsgruppen findet eine Mitwirkung an den Ausarbeitungen der Art.-29-Gruppe auch durch meine Behörde statt.

Von Apps über Smart Grid und Cookies bis zu Löschungsbegehren

Die Art.-29-Gruppe befasste sich im Berichtszeitraum mit verschiedenen Themen und gab mehrere Stellungnahmen zur EU-Datenschutzreform ab, sowohl zu einzelnen Regelungen des Entwurfs der Datenschutzgrundverordnung als auch zum Entwurf der Richtlinie für Justiz und Inneres. Technische Aspekte des Datenschutzes waren ebenso verstärkt Thema, aus diesem Bereich gab es unter anderem Stellungnahmen zu Smartphone-Apps, intelligenten Netzen und Messsystemen (Smart Grid und Smart Metering) und zur Einwilligung in die Verwendung von Cookies. Immer wieder verabschiedete die Gruppe auch Erklärungen zu Einzelfragen aus dem Bereich des internationalen Datenverkehrs. Aufgrund der Aufdeckungen der fragwürdigen Aktivitäten von Geheimdiensten veröffentlichte die Art.-29-Gruppe eine Bewertung der anlasslosen, massenhaften Überwachung von elektronischer Kommunikation durch staatliche Stellen. Das Gremium veröffentlichte daneben eine Aufstellung von Leitlinien zum Umgang mit Löschungsbegehren gegenüber Suchmaschinen nach dem EuGH-Urteil. Neben den Stellungnahmen („Working Paper“) verlautbarte die Art.-29-Gruppe ihre Auffassungen und Forderungen durch direkte Schreiben an verschiedene Stellen wie die EU-Kommission, US-Behörden, aber auch private Unternehmen wie Google.
Der Datenschutz in Europa hat mit der Art.-29-Gruppe eine vernehmbare Fürsprecherin.

Weitere Informationen:

http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm
http://ec.europa.eu/justice/data-protection/article-29/index_de.htm
www.lfd.niedersachsen.de > Themen > Wirtschaft > Internationaler Datenverkehr

Fluggastdaten: Reisende unter Verdacht

Dürfen persönliche Informationen, die Reisende gegenüber Fluggesellschaften angeben, an Sicherheitsbehörden weitergegeben und zu Sicherheitszwecken überprüft werden? Datenschützer bezweifeln nicht nur die Zulässigkeit einer anlass- und verdachtsunabhängigen Überprüfung von Fluggastdaten, sondern auch deren Nutzen für Sicherheitszwecke.

Als so genannte Passenger Name Records (PNR) oder Fluggastdaten werden neben den zur Flugabwicklung nötigen Informationen wie Name des Passagiers und geplanter Reiseverlauf auch persönliche Informationen über den Reisenden bezeichnet, so unter anderem:

- Zahlungsinformationen,
- Namen von Mitreisenden,
- Essenswünsche,
- Informationen zu gesundheitlichen Belangen,
- zum Gepäck,
- Sitzplatzinformationen.

Diese persönlichen Informationen werden von den Fluggesellschaften zur Abwicklung ihrer Geschäfte erhoben. Sicherheitsbehörden versprechen sich von der Auswertung solcher Informationen Erkenntnisse über verdächtige Personen, insbesondere im Zusammenhang mit internationalem Terrorismus, etwa über das Reiseverhalten dieser Personen oder Kontakte zu anderen verdächtigen Personen.

EU-Parlament lehnt Richtlinie ab

Fluggastdaten von europäischen Reisenden werden bereits herausgegeben an die USA und Australien, da zwischen der EU und den genannten Ländern ein entsprechendes PNR-Abkommen besteht, das als Rechtsgrundlage für diese Datenübermittlung gilt. Nachdem weitere Länder einen Bedarf an der Nutzung dieser Daten angemeldet hatten, legte die EU-Kommission bereits im Jahr 2011 einen Entwurf für eine allgemeine Richtlinie zur Nutzung von PNR zur Gefahrenabwehr und Strafverfolgung vor. Danach sollten systematisch Daten von Reisenden aus der EU heraus erfasst und für mehrere Jahre gespeichert werden. Das EU-Parlament lehnte diesen Vorschlag jedoch im Jahre 2013 endgültig ab.

Überprüfung durch den EuGH

Im Berichtszeitraum erhielt das Thema Fluggastdaten erneut Aufwind. Zunächst wurde ein geplantes PNR-Abkommen mit Kanada im Juni 2014 zwar von der EU-Kommission verhandelt und unterzeichnet, aber wiederum nicht vom EU-Parlament anerkannt; stattdessen legte das Parlament im November 2014 das Abkommen zur Prüfung dem EuGH vor. Nach der Entscheidung des EuGH zur Vorratsdatenspeicherung vom April 2014 kann nicht ausgeschlossen werden, dass auch die bestehenden PNR-Abkommen hinfällig sind. Dennoch drängen die Mitgliedstaaten, allen voran Großbritannien, weiterhin auf eine Regelung zur Nutzung von Fluggastdaten. Auch Russland, Mexiko, Südkorea und die Vereinigten Emirate fordern die Herausgabe der Daten von Personen, die per Flugzeug in ihre Länder einreisen. Nur mit Mühe konnte vereinbart werden, dass Reisende weiterhin in diese Länder einreisen oder sie überfliegen dürfen, ohne ihre Daten herausgeben zu müssen. Immer steht der Abschluss von als Rechtsgrundlage dienender internationaler Abkommen im Raum. Das EU-Parlament hat jedoch bisher deutlich gemacht, dass es solche Regelungen nicht mittragen wird.
Nach den Terroranschlägen im Januar 2015 hat das Thema erneute Brisanz erfahren. Erneut werden in den europäischen Gremien Überlegungen angestellt, die Fluggastdaten zur Auswertung für Sicherheitszwecke zu nutzen. Das Thema bleibt ein Dauerbrenner.

Verbindliche konzernweite Regelungen: Zahl der Anträge auf Binding Corporate Rules nimmt zu

Der Gebrauch von konzernweiten Regelungen zum Datenschutz durch multinationale Unternehmen hat im Berichtszeitraum erneut zugenommen. Neu hinzugekommen ist die Möglichkeit, Binding Corporate Rules (BCR) für Auftragsdatenverarbeiter zu verwenden.

BCR sind ein Instrument zur Durchführung von internationalen Datenübermittlungen. Ein international tätiges Unternehmen gibt sich selbst Datenschutzregelungen, die konzernweit gelten sollen. Entsprechen diese Regelungen den Grundsätzen der Europäischen Datenschutzrichtlinie, werden die BCR von den Aufsichtsbehörden anerkannt und können als rechtliche Grundlage für einen Datentransfer ins Ausland genutzt werden.

Niedersachsen erstmals federführend

Im Berichtszeitraum wurden erneut mehrere Anträge auf Anerkennung von BCR gestellt. Dies ist offenkundig der Zunahme von über die Grenzen hinausgehenden Datenströmen geschuldet. Im Jahr 2014 war ich erstmalig als federführende Aufsichtsbehörde in einem europaweiten Verfahren zur Anerkennung von konzernweit verbindlichen Datenschutzregelungen eines großen in Niedersachsen ansässigen Industrieunternehmens tätig. Unter Beteiligung der französischen Aufsichtsbehörde als Co-Prüferin prüfte ich umfassend die BCR im Hinblick auf ihre Vereinbarkeit mit den Vorgaben der Datenschutzrichtlinie 95/46/EG, unter anderem die Einhaltung der Betroffenenrechte, die Vornahme angemessener technisch-organisatorischer Maßnahmen oder die Übernahme der Haftung bei Rechtsverstößen. Sodann wurde das europäische Kooperationsverfahren eingeleitet, hierbei werden auch die anderen betroffenen europäischen Aufsichtsbehörden beteiligt. In mehreren Beratungsgesprächen diskutierte ich die Anmerkungen und Änderungswünsche mit dem Unternehmen und passte die Regelungen der BCR an die Vorgaben an. Nach Abschluss des europaweit geltenden Kooperationsverfahrens gelten die BCR auch für die anderen europäischen Aufsichtsbehörden als anerkannt.

Neu: BCR für Auftragsdatenverarbeiter

Cloud Computing, soziale Netzwerke, ausgelagerte Datenzentren etc. erfordern neue Lösungen zum internationalen Datenverkehr. Nachdem wiederholt Forderungen aus der Wirtschaft nach einem Mittel zur Vereinfachung der Anwendung solcher Dienstleistungen laut geworden waren, wurde im Berichtszeitrum das Rechtsinstrument der BCR für Auftragsdatenverarbeiter (Processor Binding Corporate Rules – PBCR) entwickelt. Diese Variante der unternehmensinternen Datenschutzregelungen dient der Regelung von Übermittlungen von personenbezogenen Daten, die zunächst an einen Auftragsdatenverarbeiter transferiert werden und anschließend von einem Unterauftragsdatenverarbeiter weiterverarbeitet werden. Die PBCR werden als Anhang dem zwischen dem Auftraggeber und dem Auftragnehmer vereinbarten Auftragsdatenverarbeitungsvertrag beigefügt. Der Auftraggeber bleibt auch im Verhältnis zum Unterauftragnehmer verantwortliche Stelle und ist daher auch befugt, die Anerkennung der PBCR bei den zuständigen Datenschutzbehörden zu beantragen. Der wesentliche Inhalt der PBCR ist in einem Arbeitspapier der Datenschutzbehörden festgehalten.

Weitere Informationen:

www.lfd.niedersachsen.de
> Themen
> Wirtschaft
> Internationaler Datenverkehr

10. Technisch-organisatorischer Datenschutz

10.1 Internet

Wegweisendes EuGH-Urteil zum „Recht auf Vergessenwerden“: Löschanspruch bei Suchmaschinen stärkt den Datenschutz

Der Betreiber einer Internetsuchmaschine ist bei personenbezogenen Daten, die auf von Dritten veröffentlichten Internetseiten erscheinen, für die von ihm vorgenommene Verarbeitung verantwortlich. Ihn trifft unter bestimmten Umständen auch eine Pflicht, die Auffindbarkeit von Webseiteninhalten mit personenbezogenen Daten durch Sperrung in oder Entfernung aus seinen Indizes zu erschweren. Mit diesem Grundsatzurteil des Europäischen Gerichtshofes (EuGH) vom 13. Mai 2014[1] hat der Datenschutz eine wichtige Stärkung erfahren.

Die Namenssuche in Suchmaschinen kann erhebliche Auswirkungen auf die Persönlichkeitsrechte haben, denn mit Suchmaschinen lassen sich bekanntlich weltweit in Sekundenschnelle detaillierte Profile von Personen erstellen. Im Alltag ist sich dabei kaum jemand bewusst, dass bei jeder einzelnen Suchanfrage beispielsweise bei Google-Search nach einem einzelnen oder nach kombinierten Suchbegriffen die Höchstleistung eines oder mehrerer der 19 Google-Rechenzentren[2] weltweit, die globale Netzinfrastruktur des Internet, die äußerst schnellen Google-MapReduce-Algorithmen sowie bis zu 1000 parallel arbeitende Einzelrechner beteiligt sind. Als Richtwert für die Antwortzeit aus der Sicht des Nutzers strebt der Betreiber eine halbe Sekunde oder weniger an. Am Ende ermöglicht dieser Aufwand die fast endlos mögliche Recherche in alle personenbezogenen Informationen hinein, die vielleicht längst vergessen geglaubt waren. Der EuGH hat auch erkannt, dass von der Indexierung von personenbezogenen Informationen eine erhebliche Aussagekraft ausgeht. Bieten Suchmaschinen-Verzeichnisse keinen Treffer, wird auch die Quelle der Information auf Milliarden möglichen Servern nicht leicht gefunden.

1 Urteil des EUGH vom 14. Mai 2014: http://curia.europa.eu/juris/documents.jsf?num=C-131/12
2 Siehe Website der Google Inc. mit Informationen über die „Google Data centers“ https://www.google.com/about/datacenters/gallery/

und Telemedien

Der Fall

Google Spain hatte es abgelehnt, einen solchen Sucheintrag 2010 auf Anordnung der Datenschutzaufsicht zu löschen. Der Betroffene, ein spanischer Staatsbürger, hatte Beschwerde bei der spanischen Datenschutzagentur Agencia Española de Protección de Datos (AEPD) gegen die La Vanguardia Ediciones SL, die Herausgeberin einer spanischen Tageszeitung, sowie gegen Google Spain und Google Inc. erhoben. Er machte geltend, bei Eingabe seines Namens in die Suchmaschine des Google-Konzerns („Google Search") würden den Internetnutzern in der Ergebnisliste Links zu zwei Seiten der Tageszeitung La Vanguardia von Januar und März 1998 mit veralteten Informationen zu seiner Person angeboten. Der Betroffene beantragte, die Zeitungsherausgeberin anzuweisen, entweder die betreffenden Seiten zu löschen oder so zu ändern, dass die ihn betreffenden personenbezogenen Daten dort nicht mehr angezeigt würden, oder zum Schutz dieser Daten von bestimmten, von den Suchmaschinen zur Verfügung gestellten technischen Möglichkeiten Gebrauch zu machen. Er beantragte außerdem, Google Spain oder Google Inc. anzuweisen, ihn betreffende personenbezogene Daten zu löschen oder zu verbergen, so dass diese weder in den Suchergebnissen noch in den Links zu La Vanguardia erschienen.

Die AEPD lehnte den Antrag bezüglich der Zeitung ab, gab jedoch dem Löschanspruch gegenüber Google Inc. und Google Spain statt und forderte diese beiden Gesellschaften auf, die erforderlichen Maßnahmen zu ergreifen, um die betreffenden Daten aus ihrem Index zu entfernen und den Zugang zu ihnen in Zukunft zu verhindern. Google Spain und Google Inc. erhoben daraufhin beim spanischen Gericht Audiencia Nacional (Spanien) zwei Klagen auf Aufhebung der Entscheidung der AEPD. Dieses Gericht sah grundsätzliche Fragen zur Auslegung des Unionsrechts tangiert und legte dem EuGH eine Reihe von Fragen zur Vorabentscheidung vor.

Charta der Grundrechte

Der EuGH hat sich daraufhin mit folgenden Fragen der Rechtsangleichung in den EU-Mitgliedstaaten sowie mit Begriffsklärungen zum Datenschutz befasst und dabei Art. 7 und 8 der Charta der Grundrechte der Europäischen Union sowie die Richtlinie 95/46/EG (Art. 2, 4, 12 und 14) wie folgt zugrunde gelegt:

- Art. 2 Richtlinie 95/46 des Europäischen Parlaments und des Rates, Begriffsklärung und Rechtsangleichung: „Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten";
- Art. 4 Richtlinie 95/46, Rechtsangleichung: „Anwendbares einzelstaatliches Recht: Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird";
- Art. 12 Buchst. b) und Art. 14 Abs. 1 Buchst. a) Richtlinie 95/46: „Recht der betroffenen Person auf Zugang zu den personenbezogenen Daten und Widerspruch gegen ihre Verarbeitung; Recht, die Entfernung der Links zu Internetseiten aus der Ergebnisliste zu verlangen sowie die Voraussetzungen";
- Art. 12 und 14 Richtlinie 95/46: „Mit einer Suchmaschine anhand des Namens einer Person durchgeführte Suche; Anzeige einer Ergebnisliste; Recht, zu verlangen, dass diese Information der breiten Öffentlichkeit nicht mehr zur Verfügung gestellt wird".

Die Leitsätze des Urteils

Das Urteil des EuGH vom 13. Mai 2014 (Az: C-131/12) stellt fest:

- Der Betreiber einer Suchmaschine nimmt eine Datenerhebung im Sinne der Richtlinie vor, indem er automatisch, kontinuierlich und systematisch im Internet veröffentlichte Informationen aufspürt. Es sind Daten, die der Betreiber dann mit seinen Indexierprogrammen „ausliest", „speichert" und „organisiert".
- Diese Vorgänge, die in der Richtlinie ausdrücklich und ohne Einschränkung genannt sind, sind nach Ansicht des Gerichtshofs als „Verarbeitungen" anzusehen, unabhängig davon, ob der Suchmaschinenbetreiber sie unterschiedslos auch auf andere Informationen als personenbezogene Daten anwendet.
- Sie sind auch als Verarbeitung anzusehen, wenn sie ausschließlich Informationen enthalten, die genauso bereits in den Medien veröffentlicht worden sind.
- Der Suchmaschinenbetreiber ist als im Sinne der Richtlinie für die Verarbeitung „Verantwortlicher" einzustufen, da er über die Zwecke und Mittel einer solchen Verarbeitung entscheidet.
- Diese Verarbeitung durch den Suchmaschinenbetreiber erfolgt zusätzlich zu der des Herausgebers einer Website. Deshalb hat er in seinem Verantwortungsbereich im Rahmen seiner Befugnisse und Möglichkeiten dafür zu sorgen, dass seine Tätigkeit den Anforderungen der Richtlinie hinsichtlich des Grundrechtsschutzes entspricht.
- Zum räumlichen Anwendungsbereich der Richtlinie: Weil es sich bei Google Spain um eine Tochtergesellschaft von Google Inc. in Spanien und somit eine „Niederlassung" im Sinne der Richtlinie handelt, und da diese die Aufgabe hat, in dem betreffenden Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine, mit denen deren Dienstleistung rentabel gemacht werden soll, und diesen Verkauf selbst zu sorgen, handelt es sich um eine Ausführung der Datenverarbeitung im Sinne der Richtlinie „im Rahmen der Tätigkeiten" dieser Niederlassung.
- Den Suchmaschinenbetreiber trifft unter bestimmten Voraussetzungen die Pflicht, Links zu von Dritten veröffentlichten Internetseiten mit Informationen über diese Person zu entfernen. Eine solche Verpflichtung kann auch bestehen, wenn der betreffende Name oder die betreffenden Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden, gegebenenfalls auch dann, wenn ihre Veröffentlichung dort als solche rechtmäßig ist.

- Die Leistung der Suchmaschinen ermöglicht es jedem Internetnutzer, einen strukturierten Überblick über die zu einer Person im Internet verfügbaren Informationen und potenziell zahlreiche Aspekte des Privatlebens zu erhalten. Ohne die Suchmaschine hätten die Daten nicht oder nur sehr schwer miteinander verknüpft werden können, so aber ist ein mehr oder weniger detailliertes Profil der gesuchten Personen erstellbar.
- Wegen seiner potenziellen Schwere kann ein solcher Eingriff nach Ansicht des Gerichtshofs nicht allein mit dem wirtschaftlichen Interesse des Suchmaschinenbetreibers an der Verarbeitung der Daten gerechtfertigt werden.
- Hier hat daher ein angemessener Ausgleich zwischen dem (öffentlichen) Interesse am Zugang zu der Information und den Grundrechten der betroffenen Person, insbesondere des Rechts auf Achtung des Privatlebens und des Rechts auf Schutz personenbezogener Daten, zu erfolgen.
- Zum Recht auf „Vergessenwerden" ist im Einzelfall zu prüfen, ob ursprünglich rechtmäßige Verarbeitungen sachlich richtiger Daten im Laufe der Zeit nicht mehr den Bestimmungen der Richtlinie entsprechen. Dies kann der Fall sein, wenn die Daten in Anbetracht aller Umstände des Einzelfalls, insbesondere der verstrichenen Zeit, den Zwecken, für die sie verarbeitet worden sind, nicht entsprechen, dafür nicht oder nicht mehr erheblich sind oder darüber hinausgehen.

Die Auswirkungen

Eine Person kann sich also, wenn bei einer anhand ihres Namens durchgeführten Suche in der Ergebnisliste ein Link zu einer Internetseite mit Informationen über sie angezeigt wird und es nicht mehr aktuelle oder relevante Informationen sind, unmittelbar an den Suchmaschinenbetreiber wenden, um unter bestimmten Voraussetzungen die Entfernung des Links aus der Ergebnisliste zu erwirken. Wenn dieser ihrem Antrag nicht entspricht, kann sich die betroffene Person an die zuständigen Stellen wenden. Der EuGH hat mit diesem Urteil eine für manche überraschende Entscheidung getroffen, die eine wichtige Stärkung der individuellen Persönlichkeitsrechte mit teilweisem Vorrang vor dem Veröffentlichungsrecht mit sich brachte.

Einheitliche Anwendungspraxis in Deutschland sinnvoll

In einer Ad-hoc-Arbeitsgruppe stimmten sich am 5. Juni 2014 Vertreter der Datenschutzbehörden unter Federführung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) darüber ab, wie künftig mit Eingaben verfahren werden soll, um eine sachgerechte und zügige Bearbeitung im Sinne der Rechtssicherheit zu gewährleisten. Dabei wurden die Tragweite und die Auswirkungen des Urteils erörtert, denn bei allen Datenschutzbeauftragten trafen und treffen zunehmend Eingaben ein, die sich auf die EuGH-Entscheidung beziehen und Löschansprüche mit unterschiedlichsten Begründungen und Abwägungssachverhalten geltend machen.

Reaktion und Maßnahmen von Google

Google etablierte am 29. Mai 2014 ein Verfahren, bei dem standardisiert Anträge als Webformular[3] auf Entfernung aus den Indizes gestellt werden können. Google prüft dann nach einheitlichen Kriterien[4] und ist dabei an die Vorgaben des EUGH gebunden. Sofern Google nach Prüfung entscheidet, eine Internetadresse, die so genannte URL, nicht aus den Suchergebnissen zu entfernen, kann die betroffene Person eine Überprüfung dieser Entscheidung durch eine Datenschutzaufsichtsbehörde beantragen. Dieses Verfahren ist angesichts der Fallzahlen praktikabel, darf aber nicht darüber hinwegtäuschen, dass sich nach den geltenden Bestimmungen des Bundesdatenschutzgesetzes und des Niedersächsischen Datenschutzgesetzes tatsächlich jede Person an die Aufsichtsbehörde wenden kann, ohne formal diese bei Google festgelegte Prozedur einhalten zu müssen. Allerdings würde dies das Verfahren praktisch nicht beschleunigen, und den Betroffenen wäre es in beiden Verfahrensvarianten ohnehin möglich, eine Überprüfung durch die Aufsichtsbehörde zu beantragen.
Google gibt inhaltlich an, diese Vorgehensweise auf die Löschung von Ergebnissen aus seinen Suchangeboten wie der Google-Suche, Bildersuche, Videosuche und Google News anzuwenden. Google hat nach eigenen Angaben (Zwischenstand 9. Oktober 2014)[5] seit dem Urteil des EuGH vom 13. Mai 2014 bis zum Oktober 2014 insgesamt 144.907 Anträge erhalten, die sich auf das Entfernen von 497.507 Internetlinks, also URL-Adressen, aus dem Google-Suchindex beziehen. Davon seien 41,8 Prozent entfernt und 58,2 Prozent nicht entfernt worden. Auch in meiner Behörde gingen im Berichtszeitraum einige Eingaben und Beschwerden ein, die jedoch zuständigkeitshalber an den HmbBfDI abzugeben waren, in dessen Bundesland die nach dem EuGH-Urteil als Niederlassung einzustufende Google Germany GmbH[6] ihren Sitz hat.

Google-Löschbeirat auf der Suche nach Kriterien und geregelten Abläufen

Google richtete Anfang Juli 2014 einen „Experten-Beirat für Google zum Recht auf Vergessenwerden" ein, den so genannten Löschbeirat[7], der sich mit den Kriterien befassen soll, die in Anwendung der Vorgaben des EuGH-Urteils bei Anträgen beachtet werden müssen. Der Arbeitstitel lautet: „Wie kann das Recht einer Person auf Vergessenwerden mit dem Recht der Öffentlichkeit auf Information abgewogen werden?". Vom 9. September bis 4. November 2014 führte das Gremium sieben öffentliche Sitzungen in verschiedenen Hauptstädten von Mitgliedsstaaten durch. Bis Ende 2014 lag der Abschlussbericht noch nicht vor.

---

3 Google, standardisierter Antrag als Webformular: https://support.google.com/legal/contact/lr_eudpa?product=websearch

4 Googles Entscheidungskriterien für die Entfernung der Einträge: http://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=de#how_does_googles_removals

5 Google Transparenzbericht (Transparency Report) http://www.google.com/transparencyreport/removals/europeprivacy/; Nachtrag nach Redaktionsschluss zu aktualisierten Zahlen auf dieser Seite, Stand 16. Juni 2015: Die Gesamtzahl der URLs, deren Entfernung von Google geprüft wurde: 982.552 URLs, Gesamtzahl der Ersuchen, die bei Google eingegangen sind: 270.493 Ersuchen

6 Die Google Germany GmbH in Hamburg ist nach eigenen Angaben (https://www.google.de/intl/de/about/careers/locations/hamburg/) das größte Büro in Deutschland, in dem übersetzt „ein bisschen von allem, von Marketing und Vertrieb, rund um Engineering und IT" praktiziert wird. Und weiter: „Wir sind Online-Sales-Experten, helfen großen deutschen Unternehmen und Werbetreibenden, ihre Geschäfte über Plattformen wie AdWords und AdSense aufzubauen. Unsere Marketing- und Kommunikationsteams erstellen deutschsprachige Kommunikationskampagnen für unsere Produkte." Damit sind die Kriterien der vom EuGH definierten Niederlassung erfüllt.

7 Der von Google berufene „Experten-Beirat für Google zum Recht auf Vergessenwerden" („Löschbeirat") mit Dokumentation und Zusammensetzung: https://www.google.com/intl/de/advisorycouncil/

Ungleichgewicht der Rechte

Die EuGH-Richter haben Google in Europa nunmehr ein Handlungsfeld abgesteckt, auf dem die Daten im virtuellen Raum nicht mehr grenzenlos vermarktet werden dürfen. Die Richter haben dabei mit Blick auf den Einzelnen ein Ungleichgewicht der Rechte und Chancen in der Welt der auf ewig im Netz verfügbaren Daten erkannt. Die Segnungen des Internetzeitalters bringen inzwischen für nahezu jeden Menschen tatsächlich auch Unwägbarkeiten mit sich und befördern auch den eigenen Kontrollverlust von global „vagabundierenden" Informationen. Denn manche Zusammenhänge, die sich über Suchmaschinen herstellen lassen, kommen sogar ohne Zutun des Betroffenen zustande. Diese Informationen und die jedem zugänglichen oder erzeugbaren Korrelationen unterschiedlichster Einzelquellen sind in der Praxis auch der beliebigen Bewertung und Nutzung durch Einzelpersonen, Regierungen, Medien, Organisationen und Werbetreibende, aber auch Kriminelle ausgesetzt.
Der EuGH ist diesem Umstand gerecht geworden und hat das zweifellos existierende aber oft überhöht dargestellte öffentliche Interesse am Informationszugang und des daraus abgeleiteten überhöht bewerteten Nutzens in der Wertung abgesenkt und korrigiert. Gleichzeitig hat der EuGH die Rechte- und Machtbalance zwischen mächtigen globalen Wirtschaftsunternehmen und dem einzelnen Grundrechtsträger berichtigt. Im Ergebnis hat das Gericht dem bisweilen ohnmächtigen Individuum und seinem Recht auf Privatsphäre und auf Selbstbestimmung über die eigenen Daten einen deutlichen Bedeutungsschub verschafft.
Google hat das Urteil kritisiert – was nicht überrascht. Wenn der Chefjustiziar von Google Inc. darüber Klage führt[8], dass der Abwägungsprozess zwischen Informationszugang und Datenschutz sehr schwierig sei, ist dies bei sehr speziellen Fällen zwar ohne Frage zutreffend, aber keineswegs unlösbar und schon gar nicht zu bedauern. Es geht nach meiner Überzeugung für die Grundrechtsträger vielmehr um das Zurückgewinnen von längst verloren geglaubtem Terrain gegenüber den großen Datensammlern oder zumindest um die korrigierte Grenzziehung in der Frage, was als Tabu der Datenverwendung bewertet werden muss und auch durchsetzbar wird.

Datenschutzkonferenz formuliert Anforderungen an die Suchmaschinenanbieter

Nach der Zusammenkunft der Ad-hoc-Arbeitsgruppe am 5. Juni 2014 und der Herbstsitzung des Arbeitskreises Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) am 2. und 3. September 2014 wurde deutlich, dass die Ergebnisse des Erfahrungsaustausches mit Blick auf die Stärkung des Datenschutzes für die Betroffenen zusammengefasst und durch eine Entschließung öffentlich kommuniziert werden mussten. Die 88. DSK verabschiedete daher am 8./9. Oktober 2014 die „Entschließung zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen"[9] und bezeichnete dies, bezogen auf die grundrechtliche Wirkung des EuGH-Urteils, als einen „fundamentalen Beitrag zum Schutz der Persönlichkeitsrechte im Internet". Aus der Aufsichts- und Beratungspraxis ist es allen Datenschutzbeauftragten hinlänglich bekannt, dass oftmals nicht nur verfügbare Inhalte im Netz, sondern auch die darauf referenzierenden Indexeinträge mit Personenbezug oder ganze Profile zu Personen über eine unbegrenzte Zeit hinweg abrufbar bleiben.

8 FAZ, 10. Juli 2014, Gastbeitrag des Chefjustiziars von Google Inc., David Drummond, in der Frankfurter Allgemeinen Zeitung: http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/google/google-sucht-nach-balance-fuer-loeschantraege-13038864-p2.html?printPagedArticle=true#pageIndex_2

9 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. und 9. Oktober 2014 in Hamburg: „Zum Recht auf Sperrung von Suchergebnissen bei Anbietern von Suchmaschinen"; http://www.lfd.niedersachsen.de/download/91017

Sie können dann zu sozialen und wirtschaftlichen Nachteilen für die Betroffenen führen, die mitunter ein Leben lang mit früheren tatsächlichen oder vermeintlichen Verfehlungen konfrontiert bleiben. Künftig bleiben die Betroffenen daher nicht nur darauf angewiesen, ihre Ansprüche unmittelbar gegenüber den Informationsanbietern zu verfolgen, die häufig nur schwer oder auch gar nicht zu realisieren sind. Vielmehr stellt das Urteil nun klar, dass die Betreiber von Suchmaschinen ein Recht Betroffener auf Sperrung von Suchergebnissen umzusetzen haben.

Suchergebnisse unterliegen kommerziellen Interessen

Die DSK ergänzte diese Feststellungen um einen Aspekt, der für die gesellschaftliche Debatte um den Grundrechtsschutz nicht übersehen werden darf: Zu Recht wird in der Debatte auf die erhebliche Macht der Anbieter von Suchmaschinen hingewiesen, über die Veröffentlichung von Suchergebnissen zu entscheiden. Diese Macht hat der EuGH jetzt beschnitten. Tatsächlich haben Inhalteanbieter keinen Rechtsanspruch am Nachweis ihrer Inhalte durch Suchmaschinen. Anbieter von Suchmaschinen sind keine neutralen Sachwalter der Informationsgesellschaft, sondern kommerziell handelnde Wirtschaftsunternehmen. Welche Suchergebnisse den Nutzern angezeigt werden, bestimmt sich damit jedenfalls auch nach den kommerziellen Interessen von Suchmaschinen und ihren Vertragspartnern. Darüber hinaus unterlagen Suchmaschinen auch bereits vor der Entscheidung des EuGH bei der Gestaltung der Suchergebnisse äußeren Beschränkungen, zum Beispiel durch das Urheberrecht. Mit dem Urteil wird erstmals klargestellt, dass Suchmaschinen neben diesen Erwägungen jetzt endlich auch die Grundrechte der Betroffenen zu berücksichtigen haben.
Zur Umsetzung der durch das Urteil geforderten Erwägungen weist die Datenschutzkonferenz auf folgende wichtige Praxisgrundsätze hin:

- Suchmaschinenanbieter müssen die Suchergebnisse bei einem begründeten Widerspruch angesichts der globalen Wirkung des Internet und des universellen Schutzbedarfes des Einzelnen vor unberechtigter Verbreitung personenbezogener Daten weltweit unterbinden.
- Suchmaschinenbetreiber müssen regelmäßig die Rechte der Betroffenen gegen die Interessen der Öffentlichkeit an einem freien und umfassenden Informationszugang im Einzelfall abwägen und auf die Schwere der Persönlichkeitsrechtsbeeinträchtigung, die Stellung des Betroffenen im öffentlichen Leben sowie den zeitlichen Ablauf zwischen der Veröffentlichung und dem Antrag des Betroffenen beim Suchmaschinenbetreiber abstellen.
- Die Entscheidung über die Verbreitung von Suchergebnissen, die Umsetzung von Widersprüchen und die Abwägungsentscheidung mit dem öffentlichen Interesse treffen zunächst die Suchmaschinenbetreiber. Die Kontrolle dieser Entscheidungen obliegt den jeweiligen Aufsichtsbehörden für den Datenschutz oder den staatlichen Gerichten. Alternative Streitbeilegungs- oder Streitschlichtungsverfahren dürfen das verfassungsmäßige Recht der Betroffenen auf eine unabhängige Kontrolle durch die dafür vorgesehenen staatlichen Institutionen nicht beschneiden.
- Eine Befugnis der Anbieter von Suchmaschinen, Inhaltsanbieter routinemäßig über die Sperrung von Suchergebnissen zu informieren, besteht nicht. Dies gilt auch dann, wenn die Benachrichtigung nicht ausdrücklich den Namen des Betroffenen enthält.

Marktmonopol Suchmaschine? Die Netzgemeinde hat es selbst in der Hand …

Das geflügelte Wort „ich google das mal schnell" zeigt, dass das US-Unternehmen Google Inc. den Suchmaschinenmarkt seit vielen Jahren dominiert. In Deutschland nutzt fast jeder Google. Statistischen Angaben zufolge[10] stieg der Marktanteil von 91,2 Prozent im Jahr 2014 auf 94,84 Prozent im Jahr 2015). Auf Platz 2 steht Bing mit 2,59 Prozent. Hier wird deutlich, dass ein Wettbewerb praktisch kaum noch stattfindet, obwohl es kostenfreie, datenschutzfreundliche, nicht-trackende und dabei nicht weniger zielführende Suchmaschinen wie beispielsweise metager.de, ixquick.com oder startpage.com gibt. Mit diesen Marktanteilen hat sich eine erhebliche Monopolisierung entwickelt, die durch Unkenntnis der Alternativen, durch Voreinstellung im Browser, durch Bequemlichkeit oder durch schlichte Gewohnheit der Nutzer entstanden ist und in der Folge durch extensive und exklusive Nutzung nur noch dieses Marktführers durch viele Nutzer weiter verstärkt wird.

… und kann mehr für den Selbstdatenschutz tun

Die Monopolisierung hat aber nicht nur Wettbewerbsauswirkungen im volkswirtschaftlichen Sinne, sondern erzeugt auch eine faktische Monopolstellung über die Informationshoheit. Die Suchmaschine, die zu rund 95 Prozent aufgerufen wird, kann auch durch intransparentes Ranking nach eigenen Regeln die zuvorderst angebotenen Treffer im Netz setzen und damit bestimmen, was am wahrscheinlichsten und am häufigsten aufgerufen wird. Weiter hinten platzierte Treffer müssen nicht weniger relevant sein, können aber bewusst aus betriebswirtschaftlichen Gründen diesen hinteren Rankingplatz erhalten haben, weil anderen ein höherer Stellenwert zugestanden wird. Unbemerkt für den suchenden Internetnutzer wird also Einfluss darauf genommen, was angeblich als relevant anzusehen ist. Anderes bleibt im ungünstigsten Fall unsichtbar.
Weitgehend unbekannt ist, dass mit Metasuchmaschinen eine Suchanfrage auf mehrere Suchmaschinen abgesetzt werden kann und die bei der Metasuchmaschine eingesammelten Ergebnisse nach Doublettenbereinigung in völlig anderen Rankings erscheinen können. Das Trefferbild kann also durch Einbeziehung weiterer Quellen bereichernd sein. Nicht zuletzt bieten andere Suchmaschinen den datenschutzfreundlichen Vorteil, dass die Abfrage über eine verschlüsselte Verbindung übermittelt wird und der Suchmaschinenbetreiber auf jegliches Tracking (IP-Nummern, Browser Fingerprinting usw.) verzichtet. Die Internetnutzer haben es also tatsächlich auch selbst in der Hand, ob sie die Datensammler oder die datenschutzfreundlichen Alternativen unterstützen wollen.

10 Statista GmbH, Hamburg, Suchmaschinenverteilung in Deutschland im Jahr 2015 im Vergleich zu 2014 http://de.statista.com/statistik/daten/studie/167841/umfrage/marktanteile-ausgewaehlter-suchmaschinen-in-deutschland/

Mobile Endgeräte:
Trackende Datenschnüffler und allwissende Verräter

Wird heute von mobilen Endgeräten gesprochen, so sind damit im allgemeinen Sprachgebrauch Smartphones und Tablet-Computer gemeint, obwohl auch Notebooks, Laptops, Subnotebooks und ähnliche Gerätebauarten dazugehören, die funktional und bezüglich der Bedienbarkeit weitestgehend dem herkömmlichen Desktop-PC entsprechen. In diesem Berichtsbeitrag, der die Präventivfragen zum Selbstdatenschutz insbesondere technisch-organisatorischer Natur beleuchtet, mit denen sich meine Behörde zunehmend befasst, geht es jedoch nur um die Touchscreen-basierten mobilen Endgeräte und deren Besonderheiten hinsichtlich der Datenschutzfragen und der Datensicherheit.

Dabei sind Soft- und Hardware von Smartphones und Tablet-Computern so ähnlich, dass im Folgenden nur Smartphones betrachtet werden, auch weil in diese zusätzlich zum Vollzugang in das Internet für Datenkommunikation die klassische Telefoniefunktion integriert ist. Damit werden die Risiken, die das Telekommunikationsumfeld mit den zahlreichen Datenspuren und der Ortbarkeit (Geotracking) des Gerätes mit sich bringt, kombiniert mit den Risiken, die herkömmliche PC und ihre Betriebssysteme, Bauteile und Anwendungen aufweisen. Betrachtet man die in hochwertige Smartphones zusätzlich integrierten Sensoren und die Applikationen (Apps), die diese nutzen und andere Funktionen damit kombinieren, so ergibt sich eine extreme Vielfalt an kumulierenden und sich potenzierenden Gefahren und Risiken für die informationelle Selbstbestimmung der Nutzerinnen und Nutzer. Diese Gefahren und Risiken verstärken sich in dem Maße, je weniger die Nutzerinnen und Nutzer fachliche Kenntnisse über technische Zusammenhänge aufweisen, um darauf mit Selbstschutzmaßnahmen zu reagieren.

Risiken, kombiniert mit Risiken

Anders als bei PCs ist es bei Smartphones nicht regulär möglich, das verwendete Betriebssystem und die Software frei zu wählen. Insbesondere bei dem LINUX-basierten Betriebssystem Android von Google und dem von Apple eingesetzten Betriebssystem iOS sind die Nutzer an eine Hardware-Betriebssystem-Kombination gebunden. Dies ist besonders bedenklich, da der Marktführer Android (Marktanteil laut Strategy Analytics für das 2. Quartal 2014: 84,6 Prozent) für Sicherheitslücken besonders anfällig ist. Dies scheint vor allem auf die Sicherheitspolitik hinsichtlich der Richtlinien für die Applikations-Entwicklung zurückzuführen zu sein. So ist es beispielsweise möglich, Applikationen, die Sicherheitslücken aufweisen oder selbst als Schadsoftware konzipiert sind, in Googles Downloadshop Google Play einzustellen.
Je nach Funktion einer Applikation benötigt diese unter Umständen Zugang zu privaten Daten wie Kontakte, Standort sowie Telefonnummer. Es sind jedoch zahlreiche Apps bekannt, die deutlich mehr Berechtigungen anfordern und Daten übermitteln, als für ihre eigentliche Funktion notwendig wäre. Dies betrifft zum Teil auch Applikationen, die als Bestandteil des Betriebssystems vorinstalliert sind. Das lässt sich durch den Nutzer kaum verhindern, und die vorinstallierten Applikationen können auch nicht ohne entsprechende Berechtigungen entfernt werden. Sogar reine Datensammel-Apps – gänzlich ohne Funktion für den Nutzer – wurden bereits vorinstalliert ausgeliefert. Darüber hinaus hat Google sich die Option eingerichtet, Software ohne vorherige Nachfrage beim Nutzer zu löschen oder zu installieren. Bemerkenswert ist ebenfalls, dass Android-Smartphones häufig mit einer veralteten Version des Betriebssystems verkauft werden und die Hersteller gegenüber den Kunden keine vertraglichen Verpflichtungen eingehen, neuere Versionen zur Verfügung zu stellen.
Wesentlich restriktiver erscheinen dagegen die Sicherheitsrichtlinien bei iOS. Hier muss jede erstellte Anwendung geprüft und zertifiziert werden. Dass dies aber den Nutzer in falscher Sicherheit wiegen kann, zeigt das Beispiel des Sperrbildschirms von iOS, bei dem mehrfach Sicherheitslücken aufgefallen sind. Zudem weist jedes iOS-Gerät bis einschließlich zum iPhone 4 einen Hardwarefehler auf, der es gestattet, unautorisierten Code auszuführen.

Empfehlungen

Aktuell sind personenbezogene Daten auf mobilen Endgeräten alles andere als sicher aufgehoben. Ich empfehle den Nutzerinnen und Nutzern daher dringend, folgende Hinweise zu beachten:

- Datensparsamkeit: Speichern Sie nur die personenbezogenen Daten auf Ihrem Mobilgerät, die Sie unbedingt benötigen. Das gilt auch für Fotos.
- Applikationen: Prüfen Sie alle Applikationen, die Sie auf Ihrem Mobilgerät installieren. Klingen die verlangten Zugriffsrechte plausibel oder zu umfassend? Im Zweifel alternative Apps aussuchen, die genügsamer sind. Installieren Sie eine Analyse-App, die dabei hilft, die datenschutzfreundlichen von den datenschutzunfreundlichen Apps qualifiziert zu unterscheiden.
- Updates: Achten Sie beim Kauf Ihres Mobilgeräts unbedingt auf die herstellerseitige Unterstützung mit regelmäßigen Updates für das Betriebssystem.
- Verschlüsselung: Verschlüsseln Sie personenbezogene oder andere sensible Daten bei der Übermittlung zum Beispiel mit Open-PGP.
- WLAN: Nutzen Sie nur Ihnen bekannte und verschlüsselte Netzzugänge.

Social Media: Datenschutzbeauftragte setzen Leitplanken

Wie in den Jahren zuvor betraf auch im vergangenen Berichtszeitraum ein nicht unwesentlicher Anteil der Eingaben zu Datenschutzverstößen in sozialen Netzwerken und Foren Dienstleister, die ihren Sitz nicht in Deutschland hatten und somit auch nicht in meine örtliche Zuständigkeit fielen. Es war daher nicht verwunderlich, dass sich die 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven intensiv und insbesondere mit Blick auf den Entwurf einer Datenschutz-Grundverordnung mit dem Thema Social Media auseinandersetzte. Deutlich wurde hier Position gegen alle Versuche der Umgestaltung der europäischen Datenschutzreform bezogen, die das Ziel haben, das Grundrecht auf informationelle Selbstbestimmung zu schwächen.

Die Konferenz appellierte in ihrer Entschließung „Europa muss den Datenschutz stärken“[1] an das Europäische Parlament, den Rat und die Kommission, das europäische Datenschutzgrundrecht wirksam zu gewährleisten. Insbesondere erhob sie folgende Forderungen:

- Jedes personenbeziehbare Datum muss geschützt werden.
- Es darf keine grundrechtsfreien Räume geben.
- Einwilligungen müssen ausdrücklich erteilt werden.
- Datenverarbeiter dürfen ihre Ziele nicht eigenmächtig verändern.
- Profilbildungen müssen beschränkt werden.
- Stärkung der Eigenverantwortung der Datenverarbeiter durch betriebliche Datenschutzbeauftragte.
- Datenverarbeiter dürfen sich ihre Aufsichtsbehörde nicht aussuchen können.
- Völlige Unabhängigkeit der Aufsichtsbehörden auch gegenüber der Kommission.
- Grundrechtsschutz braucht effektive Kontrollen.
- Hoher Datenschutzstandard für ganz Europa.

Orientierungshilfe beantwortet Fragen

Es zeichnete sich ab, dass die seit langem angekündigte Selbstregulierung der Betreiber sozialer Netzwerke aufgrund des Widerstandes großer Anbieter nicht zustande kommen würde und das Konzept der „Roten Linie“ gescheitert war. Die Konferenz forderte daher den Gesetzgeber in ihrer Entschließung „Soziale Netzwerke brauchen Leitplanken“[2] nachdrücklich auf, die noch bestehenden Gesetzeslücken schnell zu schließen. Zu diesem Themenkomplex hatten die Datenschutzbeauftragten eine Orientierungshilfe erarbeitet, die sich sowohl an Betreiber sozialer Netzwerke wendet als auch an Behörden oder Unternehmen, die ihre Aufgaben mit Hilfe dieser Netzwerke erfüllen wollen. Die Orientierungshilfe dient gleichzeitig als Anwendungshilfe für die Beratungs- und Prüfungspraxis meiner Behörde.

1 Entschließung: „Europa muss den Datenschutz stärken“ der 85. Konferenz vom 13. bis 14. März 2013 in Bremerhaven; https://ssl.bremen.de/datenschutz/sixcms/detail.php?gsid=bremen236.c.7665.de

2 Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven: „Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe ‚Soziale Netzwerke‘ vor“; Quelle http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=12992&article_id=113714&_psmand=48; Orientierungshilfe: http://www.lfd.niedersachsen.de/download/76198

Facebook: Alltagsbegleiter mit üblen Nebenwirkungen

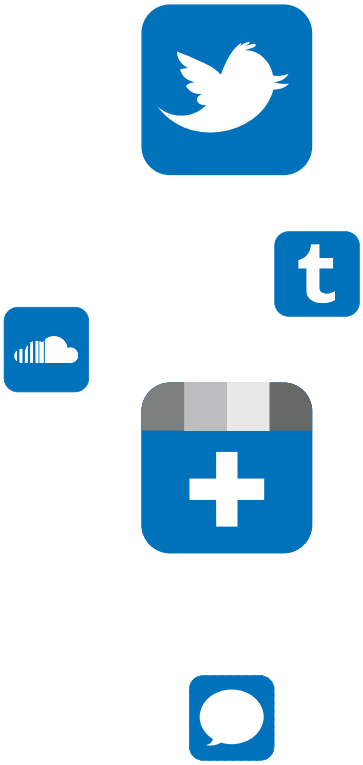
Wenngleich die wirtschaftlichen Aktivitäten der Facebook Inc. nicht in die örtliche Zuständigkeit meiner Behörde fallen, so kann ich jedoch aufgrund der weitverbreiteten Nutzung dieses Netzwerkes an diesem Thema nicht kommentarlos vorbeigehen. Für Deutschland gab Facebook im September 2013 die Zahl der Nutzer, die Facebook zumindest einmal im Monat nutzten, mit mehr als 25 Millionen an. Zudem glauben nicht nur Unternehmen, sondern auch Behörden zuweilen, ohne eine Facebook-Fanpage nicht mehr auskommen zu können. Bereits im XXI. Tätigkeitsbericht habe ich umfangreich über die datenschutzrechtlichen Fragen bei sozialen Medien im Allgemeinen und bei Facebook im Besonderen berichtet.

Auch 2013 und 2014 erhielt meine Behörde häufig telefonische und schriftliche Anfragen, die sich auf die Datenschutzpflichten des Anbieters nach dem Telemediengesetz oder auch nach dem Bundesdatenschutzgesetz (BDSG) richten. Auch öffentliche Stellen sind angesichts uneinheitlicher Rechtsprechung und tatsächlich globaler Wirkungen der Datenflüsse verunsichert, aber andererseits in dem Glauben, eine Fanpage sei zwingend notwendig.

Werbung, Werbung, Werbung

Waren im letzten Berichtszeitraum insbesondere Klarnamenzwang und Gesichtserkennung die relevanten Datenschutzthemen im Zusammenhang mit Facebook, so brachte sich das Unternehmen in den vergangenen zwei Jahren zum wiederholten Male mit datenschutzrechtlich unzulässigen Maßnahmen ins Gespräch. Die verwehrte Möglichkeit für Nutzer, Profile unter einem nach dem Telemediengesetz als zumutbar geforderten Pseudonym anzulegen, die bereits Gegenstand eines aufsichtsbehördlichen Verfahrens des schleswig-holsteinischen Landesdatenschutzbeauftragten ist, wird noch durch eine unkontrollierbare Auffindbarkeit verschärft: Bislang konnten die Nutzerinnen und Nutzer selbst bestimmen, ob das eigene Profil von allen recherchierbar sein sollte, oder ob es nur von „Facebook-Freunden“ gefunden werden sollte. Dies ist faktisch nun Geschichte: Jedes Profil kann von allen gesucht und gefunden werden. Noch problematischer ist der Umgang von Facebook mit den Nutzungsdaten, wie besonders die Beschwerden und gerichtlichen Auseinandersetzungen der österreichischen Bürgerrechtsorganisation „europe-versus-facebook“ zeigen.

Facebook erweiterte im Januar 2013 seine Suchfunktion Graph Search. Diese Erweiterung soll erneut die Reichweite für Werbezwecke deutlich erhöhen. Den Preis zahlen die Nutzerinnen und Nutzer, weil unkalkulierbar Daten ausgewertet werden. Die Funktion ermöglicht etwa Anfragen wie „Fotos meiner Freunde vor einer Datumsangabe“ oder „Lokalitäten, die meinen Freunden gefallen“, sofern sie diese Informationen mittels Facebook geteilt haben. So werden Nutzer zusätzlich zu Datenauswertern Dritter.
Solange der europäische Gesetzgeber solchen Aktivitäten keinen rechtlich tatsächlich wirksamen Riegel vorschiebt, bleibt den Nutzern von Facebook nur übrig, durch Datensparsamkeit und Zurückhaltung Schaden von sich abzuwenden.



Alternativen

Allerdings scheint die Rechnung für den hartnäckigen Grundrechteverweigerer Facebook nicht aufzugehen, denn aufgrund der großen Anzahl von Kontroversen und Kritikpunkten steigt inzwischen die Zahl jener Nutzer an, welche die Nutzung reduzieren oder ihr Facebook-Konto sogar löschen. Dies bestätigt auch eine Studie der Universität Wien aus dem Jahre 2013, bei der fast die Hälfte der Teilnehmer ihren Ausstieg mit „Sorgen um die eigene Privatsphäre“ begründete.
Möglicherweise hat sich auch inzwischen die „Idee“ Facebook – nicht zuletzt aufgrund anderer Kommunikationskanäle – überlebt. So hatte das soziale Netzwerk WhatsApp für Deutschland am 16. Januar 2014 schon mehr als 30 Millionen aktive Nutzer gemeldet. Allerdings ist die amerikanische WhatsApp Inc. nicht nur bei den Nutzerzahlen Facebook auf der Spur, sondern – wie die Mitbewerber – auch in Sachen Datenschutz. Im Mai 2012 fiel WhatsApp bei der Stiftung Warentest mit dem Urteil „sehr kritisch“ im Bereich Datenschutz durch, denn die App übermittelte alle im Handy gespeicherten Telefonnummern unverschlüsselt an den WhatsApp-Server. Erst im November 2014 wurde bekanntgegeben, dass die App mit den nächsten Updates eine Ende-zu-Ende-Verschlüsselung erhalten soll. Unter der Voraussetzung, dass es sich um eine fehlerfreie Implementierung handelt, ist dies aus meiner Sicht ein sehr begrüßenswerter Fortschritt.
Im Februar 2014 gelang es Facebook, durch Übernahme von WhatsApp zwei Schwergewichte sozialer Netzwerke zur Vergrößerung der weltweiten Marktanteile unter einem Unternehmensdach zu vereinen. Diese weitgehende Monopolisierung ist Ursache für weitere Sorgen, denn damit sinkt für Millionen Nutzerinnen und Nutzer erneut die Wahrscheinlichkeit zur Beseitigung der Datenschutzprobleme.

Orientierungshilfe für Betreiber, Behörden und Unternehmen

Die 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat am 13./14. März 2013 in Bremerhaven mit einer Entschließung[1] „Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe ‚Soziale Netzwerke‘ vor“ festgestellt, dass hier Handlungsbedarf besteht (siehe auch Seite 130). Die Konferenz for-

1 Entschließung der 85. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 13./14. März 2013 in Bremerhaven: „Soziale Netzwerke brauchen Leitplanken – Datenschutzbeauftragte legen Orientierungshilfe ‚Soziale Netzwerke‘ vor“; Quelle http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=12992&article_id=113714&_psmand=48; Orientierungshilfe: http://www.lfd.niedersachsen.de/download/76198

derte daher den Gesetzgeber nachdrücklich auf, die noch bestehenden Gesetzeslücken schnell zu schließen. Die veröffentlichte Orientierungshilfe richtet sich sowohl an Betreiber sozialer Netzwerke, als auch an Behörden und Unternehmen, die mit sozialen Netzwerken ihre Aufgaben erfüllen (wollen) oder ihre Geschäftszwecke verfolgen und soll bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. Außerhalb des Fokus liegen allerdings die privaten Nutzerinnen und Nutzer sozialer Netzwerke. Die Orientierungshilfe ist deshalb auch keine Anleitung für den datenschutzgerechten Gebrauch solcher Netzwerke. Hinweise und Anleitungen für Nutzerinnen und Nutzer derartiger Dienste werden jedoch von verschiedenen Datenschutzbehörden und anderen Einrichtungen zur Verfügung gestellt.
Angesichts der zunehmenden Bedeutung sozialer Netzwerke erinnert die Datenschutzkonferenz deren Betreiber an ihre Verpflichtung, die Einhaltung datenschutzrechtlicher Anforderungen sicherzustellen. Auch Unternehmen und öffentliche Stellen, die soziale Netzwerke nutzen, müssen diesen Anforderungen Rechnung tragen. Die Erfahrung der Aufsichtsbehörden zeigt, dass der Schutz der Privatsphäre von den Betreibern sozialer Netzwerke nicht immer hinreichend beachtet wird. Häufig vertrauen die Nutzenden den Betreibern dieser Dienste sehr persönliche Informationen an. Auch die Vielfalt der Informationen, die innerhalb eines Netzwerkes aktiv eingestellt oder über die Nutzerinnen und Nutzer erhoben werden, ermöglicht einen tiefen Einblick in deren persönliche Lebensgestaltung. Es zeichnet sich ab, dass die angekündigte Selbstregulierung für soziale Netzwerke – insbesondere auf Grund der mangelnden Bereitschaft einiger großer Netzwerk-Betreiber – den erforderlichen Datenschutzstandard nicht gewährleisten kann.
Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“ erarbeitet. Die Konferenz weist darauf hin, dass der vorhandene Rechtsrahmen zur Gewährleistung eines angemessenen Datenschutzes bei sozialen Netzwerken weiterentwickelt werden muss, insbesondere in Bezug auf

- konkrete und präzise Vorgaben zu datenschutzfreundlichen Voreinstellungen,
- zum Minderjährigenschutz,
- zur Löschungsverpflichtung bei Dritten und
- zum Verhältnis von Meinungsfreiheit und Persönlichkeitsrecht.

Ferner wird die Verantwortlichkeit für den Umgang mit Nutzungsdaten in Bezug auf Social Plug-Ins, Fanpages sowie für den Einsatz von Cookies von vielen Unternehmen und Behörden in Abrede gestellt. Der europäische und nationale Gesetzgeber bleiben aufgefordert, für die notwendige Klarheit zu sorgen und damit einen ausreichenden Datenschutzstandard zu sichern. Darauf weist die Konferenz der Datenschutzbeauftragten nachdrücklich hin.

Rechtsprechung wirft Fragen auf

Das Schleswig-Holsteinische Verwaltungsgericht verneinte am 9. Oktober 2013 mit drei Urteilen (8 A 218/11, 8 A 14/12, 8 A 37/12 eine (Mit-)Verantwortlichkeit der Nutzer hinsichtlich der mit der Eröffnung einer Fanpage ausgelösten Vorgänge der Erhebung, Verwendung und Verarbeitung personenbezogener Daten. Hintergrund des Urteils ist eine Musterverfügung, mit der das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) der Wirtschaftsakademie der Industrie- und Handelskammer (WAK) auferlegt hatte, ihre Fanpage bei Facebook zu deaktivieren. Hiergegen hatte die WAK erfolgreich beim Verwaltungsgericht Schleswig (VG) geklagt.

In zweiter Instanz urteilte das Schleswig-Holsteinische OVG[2] am 4. September 2014 nach mündlicher Verhandlung, dass Betreiber von Facebook-Fanpages in keiner Weise eine Verantwortung für die hierüber ausgelöste Verarbeitung von Nutzungsdaten bei Facebook trügen. Sie seien weder verantwortliche Stelle im Sinne des Datenschutzrechts noch als Störer verantwortlich zu machen. Derzeit steht eine Entscheidung des Bundesverwaltungsgerichtes in der Sache aus, da das ULD Schleswig-Holstein am 29. September 2014 Revision eingelegt hat.

Andererseits urteilte das Kammergericht Berlin am 24. Januar 2014 zugunsten der Verbraucherzentrale Bundesverband (vzbv). Die vzbv hatte im November 2010 Klage gegen Facebook vor dem Landgericht Berlin eingereicht, nachdem das Unternehmen nicht auf eine erneute Abmahnung des vzbv reagiert hatte. Die vzbv begründete die Abmahnung damit, dass Klauseln in den Allgemeinen Geschäftsbedingungen sowie die Datenschutzbestimmungen gegen geltende Verbraucherrechte verstießen. Hauptkritikpunkte waren der Adressbuchimport und Freundefinder sowie die Datennutzung durch Drittanbieter. Am 6. März 2012 gab das Landgericht Berlin der Klage vollumfänglich statt. Facebook legte gegen das Urteil Berufung ein. Das Kammergericht Berlin wies die Berufung von Facebook am 24. Januar 2014 ab und bestätigte damit die Rechtsauffassung der vzbv[3].

Das Gericht ließ in der mündlichen Verhandlung keinen Zweifel daran, dass für Facebook nicht irisches, sondern deutsches Datenschutzrecht gilt. In der Begründung stützte sich das Gericht neben der Rechtswahlklausel auch auf eine Stellungnahme der so genannten Artikel-29-Datenschutzgruppe aus dem Jahr 2010[4] zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“. Danach sei entscheidend, bei wem de facto die Verantwortung für die Verarbeitung der Daten liege.

Das Kammergericht ließ die Revision gegen das Urteil nicht zu. Facebook hätte aber noch die Möglichkeit, beim Bundesgerichtshof eine Nichtzulassungsbeschwerde einzulegen.

Vom Einsatz in Behörden und Kommunen wird abgeraten

Seit einigen Jahren hat meine Behörde in zahlreichen Veranstaltungen und Einzelberatungen den öffentlichen Stellen vom Einsatz der Facebook-Fanpages aus datenschutzrechtlichen und technisch-organisatorischen Gründen abgeraten. In meinem letzten Tätigkeitsbericht hatte ich über die Einzelheiten der Begründungen bereits berichtet. Insbesondere die Kommunen haben bislang diese Empfehlungen fast ausnahmslos angenommen. Auch meine Empfehlungen zum Verzicht auf den rechtswidrigen Einsatz von implementierten Social Plugins wie dem Like-Button als Fremdcode auf der eigenen Website sind von den Behörden offenbar weitestgehend flächendeckend nachvollzogen worden.

Eine vergleichbare Haltung habe ich demgegenüber auf der Ebene der Niedersächsischen Landesregierung nicht angetroffen. Auch hier ist meine Behörde sehr frühzeitig aktiv geworden. Bereits im März 2013 hat mein Amtsvorgänger der Staatskanzlei die eingangs erwähnte Entschließung der Datenschutzkonferenz des Bundes und der Länder sowie die

2 Urteil OVG Schleswig-Holstein mit Begründung: https://www.datenschutzzentrum.de/uploads/facebook/20140904-OVG-U-FBFanpageAnon.pdf; ULD-Presseinformation dazu: https://www.datenschutzzentrum.de/artikel/774-Schleswig-Holsteinisches-OVG-Rechtssicherheit-fuer-Betreiber-nicht-fuer-die-Betroffenen.html#extended

3 Urteil Kammergericht Berlin: http://zap.vzbv.de/3e8a1877-9b7d-417e-868c-44ff40e525a8/16_o_551_10_urteil_vom_06. März 2012_landgericht_berlin_anonymisiert.pdf und http://www.surfer-haben-rechte.de/content/erfolg-zweiter-runde-fuer-vzbv-kammergericht-weist-berufung-von-facebook-zurueck

4 Artikel-29-Gruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher“ und „Auftragsverarbeiter“ vom 16. Februar 2010, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_de.pdf

entsprechende Orientierungshilfe zugeleitet und damit die Erwartung verbunden, dass die Ergebnisse und Erkenntnisse ihren Niederschlag bei künftigen Entscheidungen der Landesregierung finden. Gleichwohl informierte das Wirtschaftsministerium (MW) am 29. Januar 2014 in einer Pressemitteilung über die Einrichtung einer Facebook-Fanpage. Nur wenige Monate später, nämlich im April 2014, erfuhr ich durch eigene Recherchen, dass auch das Sozialministerium (MS) zwischenzeitlich mit einer Fanpage bei Facebook vertreten war. Meine Behörde ist in beiden Fällen mit gleichlautenden Schreiben vom 17. Februar 2014 bzw. 29. April 2014 an MW und MS herangetreten und hat in diesen Schreiben unter ausführlicher Darlegung der Rechtslage um Vorlage der erforderlichen Verfahrensbeschreibungen und ggf. der Ergebnisse der diesbezüglichen Vorabkontrollen gebeten. In ihren Antwortschreiben verweigerten beide Ministerien die Vorlage dieser Unterlagen und bezogen sich zur Begründung im Wesentlichen auf das zuvor erwähnte OVG-Urteil aus Schleswig-Holstein. Ende Oktober 2014 hat mein Amtsvorgänger schließlich in einem ausführlichen Beratungsgespräch mit Vertretern der Staatskanzlei den Versuch unternommen, darauf hinzuwirken, dass von dem beabsichtigten Fanpageauftritt Abstand genommen wird. Der Ausgang war zum Ende des Berichtszeitraums noch offen

Fazit

Auch in Anbetracht des zehnjährigen Jubiläums von Facebook im Februar 2014 halte ich es für bemerkenswert, dass sich ein globales Unternehmen, das seit Geschäftsgründung 1,2 Milliarden Nutzer gewonnen hat, erfolgreich weigern kann, geltendes Recht in Deutschland zu beachten. Fragwürdig ist dieses Jubiläum auch deshalb, weil es mehr als deutlich macht, dass sich Facebook, aber auch andere soziale Netzwerke, zunehmender Beliebtheit erfreuen, ohne dass die Nutzerinnen und Nutzer noch ansatzweise eine Kontrolle über ihre Daten haben. Umso bedenklicher ist diese Situation, wenn auch öffentliche Stellen dieses Geschäftsmodell nutzen und rechtsunkundige Internetuser auf Seiten „locken“, auf denen sie vermeidbare Datenschutzrisiken eingehen. Der Stellenwert, der dem Grundsatz des rechtskonformen Verwaltungshandelns zukommt, wird auf diese Weise konterkariert.

Feuerwehreinsätze auf Facebook: Vorsicht bei der Veröffentlichung von Anschriften und Fotos

Durch mehrere Eingaben wurde ich darauf aufmerksam gemacht, dass freiwillige Feuerwehren öffentlichkeitswirksame Auftritte mit Hilfe einer Facebookseite initiiert hatten. Teilweise waren im Internet Bilder und Einsatzörtlichkeiten zu sehen, die einen unmittelbaren Personenbezug ermöglichten. In einzelnen Fällen wurde sogar die exakte Wohnanschrift mit der Hausnummer veröffentlicht, an der ein Einsatz der Feuerwehr erforderlich war. Auch wurden Bilder eines Brandobjekts in Kombination mit der Wohnadresse auf die Facebookseite hochgeladen.

Gegenüber den für den Facebookauftritt verantwortlichen Gemeinden und Landkreisen stellte ich Folgendes klar:

- Bei textlichen Informationen zu dem Einsatzgeschehen der Feuerwehr auf der Facebookseite muss noch intensiver darauf geachtet werden, dass mit den veröffentlichten Daten kein Personenbezug herstellbar ist. So dürfte es regelmäßig ausreichend sein, den entsprechenden Ortsteil des Einsatzes zu benennen und insbesondere auf Zusätze wie die Straßenbezeichnung in Kombination mit weiteren Anhaltspunkten zu verzichten.
- Das Veröffentlichen von Foto- und Videoaufnahmen einer Einsatzstelle unterliegt klaren rechtlichen Grenzen, die einer individuellen Prüfung vor einer Einstellung bedürfen. Von öffentlich zugänglichen Bereichen aus darf grundsätzlich uneingeschränkt foto- und videografiert werden; hierbei muss die „Perspektive des normalen Fußgängers“ eingehalten werden. Leistungsfähige Teleobjektive und Leitern zur Überwindung eines Zauns oder die Aufnahme durch eine Grundstückshecke oder ein Fenster verbieten sich.
- Bei der anschließenden Veröffentlichung des Materials sind die Bestimmungen des Kunst-Urheberrechtsgesetzes (KunstUrhG) in Ausformulierung des Rechts am eigenen Bild (§ 22 KunstUrhG) zwingend zu beachten. Das heißt, jede aufgenommene Person entscheidet selbst darüber, wann und in welchem Zusammenhang ihr Bild oder ihre Aufnahme zu sehen sein wird. Die Veröffentlichung eines Fotos mit einer erkennbaren Person ist nur zulässig, wenn die oder der Abgebildete ausdrücklich zugestimmt hat. Das Einverständnis muss sich auch auf den Zeitraum, den Ort und den Zweck der Veröffentlichung beziehen. Wegen des weitreichenden Charakters einer solchen Einwilligung muss die Schriftform gewählt werden. Eine erteilte Einwilligung kann jederzeit widerrufen werden; die weitere Veröffentlichung ist ab diesem Zeitpunkt unzulässig.

Ausnahmen vom Recht am eigenen Bild

§ 23 Abs. 1 KunstUrhG lässt allerdings Ausnahmen von dieser Regel zu:
„Bildnisse aus dem Bereiche der Zeitgeschichte" (§ 23 Abs. 1 Ziffer 1 KunstUrhG)
Hierzu gehören nach gängiger Rechtsprechung auch Personen der Zeitgeschichte, die eine gewisse Prominenz aufweisen und über die regelmäßig berichtet wird. Zu diesem Kreis zählen ferner offizielle Vertreter von Behörden, Einrichtungen und Unternehmen, die im dienstlichen Zusammenhang mit dem jeweiligen Feuerwehreinsatz aufgenommen werden. So dürfte es zulässig sein, Aufnahmen zu veröffentlichen, auf denen beispielsweise Feuerwehrangehörige und Polizeibeamte im Rahmen des Einsatzgeschehens erkennbar sind.
„Bilder, auf denen Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen" (§ 23 Abs. 1 Ziffer 2 KunstUrhG)
Auch identifizierbar Abgebildete müssen eine Veröffentlichung ohne ausdrückliche Einwilligung hinnehmen, wenn sie lediglich als „Beiwerk" neben einer sonstigen Örtlichkeit anzusehen sind. Eine sonstige Örtlichkeit in diesem Sinne kann auch ein Einsatzort der Feuerwehr sein. „Beiwerk" stellen Personen unter anderem dar, wenn auf dem Foto eines Einsatzgeschehens oder Verkehrsunfalles eine einzelne Person im Randbereich oder aber mehrere Personen, zum Beispiel Schaulustige, zu erkennen sind. Nach ständiger Rechtsprechung sind hier mindestens fünf Personen erforderlich.
Die weiteren Ausnahmen des § 23 Abs. 1 KunstUrhG dürften bei Einsätzen der Feuerwehr nicht von Belang sein. Entscheidend ist bei einer Veröffentlichung ferner, dass kein berechtigtes Interesse des oder der Abgebildeten verletzt wird (§ 23 Abs. 2 KunstUrhG).

Weitere Kontrollen angekündigt

Gegen die Veröffentlichung von Bild- und Videomaterial, das die genannten Maßgaben nicht verletzt, kann ich somit grundsätzlich keine Einwände vorbringen. Meine generellen Vorbehalte gegen die Nutzung sozialer Netzwerke bleiben selbstverständlich bestehen (vgl. XXI. Tätigkeitsbericht 2011–2012 – Schwerpunktthema Soziale Netzwerke, ab Seite 118).
Hiervon losgelöst bat ich die Kommunen ausdrücklich um die Beachtung der folgenden Grundsätze:

1. Die aktuellen Veröffentlichungen der Feuerwehren sind im Hinblick auf eine Personenbeziehbarkeit und die Bestimmungen des KunstUrhG zu überprüfen. Sollte ein Personenbezug herstellbar sein (insbesondere durch Bild- oder Videoaufnahmen), der nicht unter die Ausnahmebestände des KunstUrhG fällt, habe ich dazu aufgefordert, diese Veröffentlichungen zu löschen oder datenschutzkonform anzupassen.
2. Für zukünftige und aktuelle Veröffentlichungen bat ich darum, meine Ausführungen zu beachten und die Medienverantwortlichen der Feuerwehren darüber zu unterrichten. In diesem Zusammenhang könnte es sich anbieten, mit einer Handlungs- oder Dienstanweisung für die Feuerwehren den Spielraum im Zusammenhang mit Veröffentlichungen eindeutig zu definieren.
3. Die behördlichen Datenschutzbeauftragten sollten bei vorgesehenen oder erfolgten Veröffentlichungen beteiligt werden.

Die in Rede stehenden Facebookauftritte der Feuerwehren werde ich mir in Zukunft gelegentlich anschauen und hinsichtlich der Beachtung meiner aufgestellten datenschutzrechtlichen Grundsätze überprüfen.

Trackingtechnik: Browsermerkmale und Surfverhalten sind begehrtes Informationsgut

Wie in den vergangenen Jahren betrafen die im Berichtszeitraum eingegangenen Eingaben zum Datenschutz in Telemedien im Schwerpunkt die Themenfelder soziale Netzwerke, Internet-Foren sowie Direktmarketing. Bei der Prüfung von Verstößen gegen Datenschutzbestimmungen bei Telemedien musste ich leider feststellen, dass nach wie vor wenige Bürger ihre Betroffenenrechte wirklich kennen. Auch die Telemedien-Anbieter haben weiterhin bedenkliche Defizite, was die Kenntnisse von Rechten und Pflichten beim Umgang mit personenbezogenen Daten anbelangt.

Bei den Telemedienanbietern fehlte es ebenso regelmäßig an der erforderlichen Fachkunde, Telemedien sicher, also nach den Erfordernissen der Informationssicherheit angemessen auszugestalten. Oft wurde irrtümlich angenommen, dass eine Software „von Haus aus" nicht nur sicher, sondern auch datenschutzrechtlich unbedenklich sei, wenn sie nur oft genug im Internet verwendet wird oder aufgrund ihrer Popularität einen hohen Marktanteil einnimmt. Dass auch auf der eigenen Webseite eingebundene Werbung oder Funktionen zur Reichweitenmessung einen Bußgeldtatbestand erfüllen können, wussten die wenigsten Anbieter. Insbesondere derjenige, der ohne konkrete Einwilligung des Telemedien-Nutzers dessen personenbezogene Daten, wie zum Beispiel die IP-Adresse, über Dienste wie Google Analytics, Google AdSense oder den Facebook Like-It-Button in die USA übermittelt, begeht, wenn dies vorsätzlich oder fahrlässig geschieht, gemäß § 16 Abs. 2 Telemediengesetz (TMG) eine Ordnungswidrigkeit und muss mit einem Bußgeld rechnen.

Hinweise seit fünf Jahren online

Im Web-Tracking-Report 2014 des Fraunhofer SIT[1] wird festgestellt: „Unternehmen fördern den Rohstoff Daten heute in großem Stil durch Web-Tracking. Mittels Web-Tracking können dritte Parteien nichtsahnende Verbraucher im Hintergrund bei deren Internetnutzung verfolgen und somit umfangreiche Einblicke in die Interessen, Wünsche, Probleme oder den Konsum von Verbrauchern gewinnen und Profile von Verbrauchern erstellen." Diese Erkenntnis deckt sich mit den Feststellungen meiner Behörde. Es herrscht gewissermaßen eine Goldgräberstimmung auf diesem Markt der Daten. Um hier Abhilfe zu schaffen und darauf explizit hinzuweisen, welche Vorgaben für rechtskonforme Verfahren erfüllt

Orientierungshilfe für Diensteanbieter für Telemedien als Download unter: www.lfd.niedersachsen.de > Themen > Internet > Telemedien

1 Markus Schneider, Matthias Enzmann, Martin Stopczynski, Hrsg. Michael Waidner, Fraunhofer-Institut für Sichere Informationstechnologie SIT: „SIT Technical reports – Web-Tracking-Report 2014", Februar 2014; https://www.sit.fraunhofer.de/de/wtr/

sein müssen, habe ich bereits im November 2010 eine Handreichung für Anbieter von Telemedien veröffentlicht.

EU-Cookie-Richtlinie fordert seit 2002 gesetzgeberisches Handeln der Mitgliedstaaten

Cookies und verschiedene andere Technologien ermöglichen die Verfolgung des Nutzerverhaltens im Internet. Sie werden immer häufiger zur Bildung von anbieterübergreifenden Nutzungsprofilen verwendet, um Nutzern dann zum Beispiel auf sie zugeschnittene Werbung anzuzeigen. Die EU-Datenschutzrichtlinie für elektronische Kommunikation (E-Privacy-Richtlinie)[2] gestattet die Speicherung von Informationen oder den Zugriff auf Informationen, die bereits im Endgerät eines Nutzers gespeichert sind, jedoch nur, wenn der Nutzer dazu seine Einwilligung gegeben hat. Außerdem müssen die Diensteanbieter die Nutzer vor der Speicherung von Informationen mittels Cookies, Web Storage oder ähnlichen Instrumenten klar und umfassend über deren Zweck informieren. Dies gilt auch für den Zugriff auf Browser- oder Geräteinformationen zur Erstellung von sogenannten Browser Fingerprints und Device Fingerprints. Der europäische Gesetzgeber misst dem Einsatz dieser Technologien zu Recht ein hohes Gefährdungspotential für die Persönlichkeitsrechte der Nutzer bei.

Seit Jahren wird im Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Umstand kritisiert, dass das in Deutschland geltende Telemediengesetz (TMG) diese europarechtlichen Vorgaben nur unvollständig in nationales Recht umsetzt. Darauf haben die Datenschutzbeauftragten von Bund und Ländern die Bundesregierung bereits wiederholt hingewiesen. Dies hat

2 E-Privacy-Richtlinie, Art. 5 Abs. 3, Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Amtsblatt Nr. L 201 vom 31. Juli 2002 S. 0037–0047, http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32002L0058&from=DE

bisher jedoch nicht zu einer Änderung des TMG geführt. Die Bundesregierung hält vielmehr die derzeit geltenden Vorgaben des TMG für ausreichend. Diese Einschätzung ist nach übereinstimmender Auffassung der Datenschutzbeauftragten unzutreffend. So ist die europarechtlich geforderte Einwilligung bereits in den Zugriff auf in den Endgeräten der Nutzer gespeicherte Informationen (Cookies) im deutschen Recht nicht enthalten.

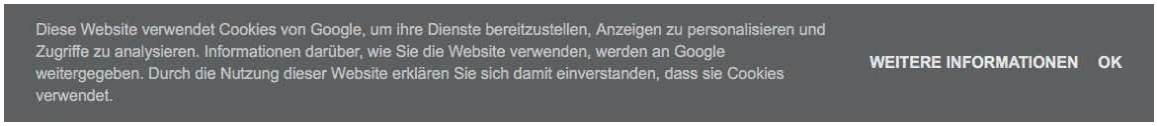
Untätige Bundesregierung

Die fortgesetzte Untätigkeit der Bundesregierung und des Gesetzgebers hat zur Folge, dass gegenwärtig die Betroffenen ihre Ansprüche zur Wahrung der Privatsphäre aus Art. 5 Abs. 3 der E-Privacy-Richtlinie gegenüber Anbietern in Deutschland, bei denen das TMG zur Anwendung kommt, nur unzureichend wahrnehmen können. Damit wird den Bürgerinnen und Bürgern faktisch ein europarechtlich vorgesehenes, wesentliches Instrument zur Wahrung ihrer Privatsphäre bei der Nutzung des Internets in den nationalen Rechtsgrundlagen und in der Folge im praktischen Vollzug vorenthalten. Gerade die Weiterentwicklung von neuen Technologien zur Sammlung und Analyse des Nutzerverhaltens im Internet macht moderne und effiziente Regelungen zum Schutz der Privatsphäre der Nutzer jedoch unabdingbar.

Entschließungsentwurf der Datenschutzkonferenz

Zum Ende des Berichtszeitraumes arbeitete der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Entschließung aus, die sich auf die fehlende Umsetzung der „Cookie-Richtlinie" bezieht. Sie soll 2015 verabschiedet werden. Diesen Zustand fehlender rechtlicher Umsetzung halte auch ich für nicht hinnehmbar. Auch in Deutschland muss die E-Privacy-Richtlinie nun ohne weitere Verzögerungen vollständig in das nationale Recht überführt werden. Dabei müssen nach meiner Überzeugung nicht nur die Minimalanforderungen der Richtlinie kodifiziert, sondern auch die Grundlage für einen umfassenden und zeitgemäßen Schutz der Persönlichkeitsrechte im Internet und unter Berücksichtigung der schnellen technologischen Entwicklungen geschaffen werden.
Neben dem altbekannten Cookie, der inzwischen nicht mehr den aktuellen Stand der Technik repräsentiert, und neben den weiterentwickelten Varianten wie Third-Party-Cookies, Flash-Cookies, Web Storage (auch DOM Storage oder Supercookies)[3] stehen inzwischen erheblich aussagekräftigere Instrumente zur Verfügung. So finden Verfahren zur Aufzeichnung des Nutzerverhaltens inzwischen auch auf anderen Endgeräten als den herkömmlichen Rechnern Anwendung. Zu nennen sind hier nicht nur aktuelle mobile Endgeräte wie Tablets und Smartphones, sondern auch Geräte der Unterhaltungselektronik wie Smart-TV, Spielekonsolen und andere Entertainmentgeräte mit Internetanschluss.

3 Flash-Cookies sind Entwicklungen zum Macromedia Flash Player des Herstellers Adobe, auch Local Shared Objects (LSO) genannt. Auf diese neuen Arten der verräterischen Spuren wurde bereits mehrfach in den Tätigkeitsberichten hingewiesen: XIX. Tätigkeitsbericht 2007–2008, Seite 51, und XX. Tätigkeitsbericht 2009–2010, Seite 129



Hinzu kommt, dass hierfür inzwischen auch Technologien in breitem Maße Anwendung finden, die von der E-Privacy-Richtlinie 2002/58/EG auch in ihrer Fassung 2009/136/EG im Wortsinne nicht mehr erfasst werden. Bei diesen Technologien brauchen Datensammlungen nicht mehr aktiv auf im Endgerät gespeicherte Informationen seitens der verantwortlichen Stelle zuzugreifen, weil diese Daten jeweils aktuell nach Aufforderung erzeugt werden, ohne dass eine Speicherung auf einem Datenträger im Sinne des § 3 IV Nr. 1 Bundesdatenschutzgesetz (BDSG) erfolgt. Dadurch ist eine Bestimmung und Wiedererkennung des Endgerätes und/oder der Nutzer allein anhand der im Rahmen der für die Kommunikation erforderlichen anfallenden Daten faktisch möglich. Zu diesen neuen aber inzwischen etablierten Verfahren des User-Trackings gehören insbesondere Methoden wie das Canvas Fingerprinting[4] oder Browserfingerprinting, mit dem über das Internetnutzungsverhalten durch zusätzliche Kombination einer Vielzahl von Merkmalen ein viel schärferes Bild des Nutzers gezeichnet wird und Nutzer somit effektiv und effizient beobachtet und analysiert werden können.

Darüber hinaus ist festzustellen, dass die Verfasser der Richtlinie 2002/58/EG der damaligen Praxis folgend vorrangig davon ausgegangen waren, dass die Aufzeichnung des Nutzungsverhaltens in personenbezogener oder pseudonymer Form ausschließlich durch den Telemedienanbieter erfolgt, so dass sich das entstandene Profil auf Aussagen zur Nutzung dieses einen Telemediums oder zumindest auf die Telemedien eines Anbieters, die vom Nutzer explizit aufgesucht wurden, beschränkt. Gegenwärtig werden Verfahren zur Auswertung des Nutzerverhaltens selbst dann, wenn diese ausschließlich für eigene Zwecke des Anbieters dienen, regelmäßig auch mit Hilfe außereuropäischer Anbieter realisiert, die diese Daten nicht im Rahmen einer Auftragsdatenverarbeitung und damit der Mandantentrennung unterfallend auswerten, sondern diese vielmehr auch für eigene Zwecke verarbeiten. Das führt dazu, dass diese Dienstleister, die in der Regel für den Nutzer nicht einmal erkennbar sind, ein umfassendes Bild über das gesamte Internetnutzungsverhalten der Betroffenen erstellen und wirtschaftlich nutzen können.

Auch wenn die in der überwiegenden Zahl der Fälle fehlende bzw. unzureichende Information im Sinne der Vorgaben der E-Privacy-Richtlinie in der alten Fassung von 2002 bereits bisher Möglichkeiten zu aufsichtsbehördlichem Tätigwerden bot, bedarf es insbesondere im Hinblick auf Trackingtechniken, die ohne den Zugriff auf gespeicherte Daten auskommen und daher auch von Art. 5 der neueren Version nicht erfasst werden, einer Anpassung des § 15 III TMG. Die Anpassung sollte nach meiner Überzeugung enthalten, dass

- die Nutzerin oder der Nutzer in einer auch für andere Geräte wie Mobiltelefone oder Fernseher geeigneten Form umfassend informiert wird,
- die Einwilligungslösung der aktuellen Fassung der Richtlinie übernommen wird und
- jegliche Form personenbezogener oder pseudonymer Profilbildung von der Regelung erfasst wird.

4 Vgl. Fachartikel heise-online: „User-Tracking: Werbefirmen setzen bereits häufig ‚nicht-löschbare' Cookie-Nachfolger ein" vom 22.2014; http://www.heise.de/newsticker/meldung/User-Tracking-Werbefirmen-setzen-bereits-haeufig-nicht-loeschbare-Cookie-Nachfolger-ein-2264381.html

Biometrische Gesichtserkennung im Internet: Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!

Die großen im Internet dominierenden Anbieter – vor allem Google und Facebook – haben seit einigen Jahren erkannt, dass Informationen zu Personen umso aussagekräftiger sind, je enger sie mit einem Gesicht der Person in Zusammenhang gebracht werden können. Die Metapher „Ein Bild sagt mehr als tausend Worte" trifft hier im besonderen Maße zu. Doch die Intention der Internetfirmen ist klar: Je realistischer das Profil erstellt werden kann, desto wertvoller ist der vermarktbare Datensatz.

Geht es den an sozialen Netzwerken (Social-Media-Plattformen) teilnehmenden Personen häufig zunächst darum, die Anonymität gerade aufzugeben, um anderen von Angesicht zu Angesicht im Netz zu begegnen, so verfolgen die mit diesen Datenmengen hantierenden Telemedienanbieter aufgrund ihrer kommerziellen Interessen ein anderes Ziel. Es geht ihnen darum, möglichst viele Daten über die Profilinhaber und Korrelationen zwischen Person und Person sowie zwischen Person und Profilmerkmalen zu erhalten. Diese Erkenntnisse schärfen das Bild der Interessen und Vorlieben der Menschen und ermöglichen damit ein passgenaues Werbeprofil, das die virtuelle Währung im Netz darstellt.

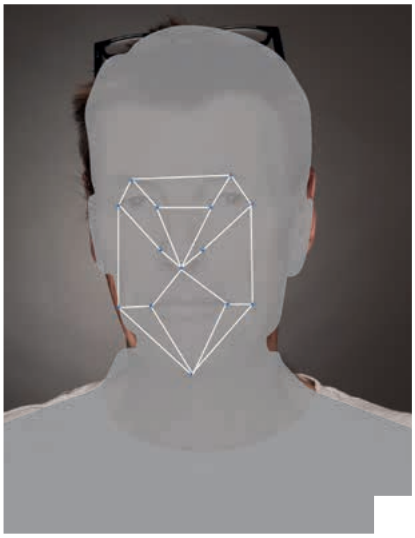
Lücken in Lebensläufen können geschlossen werden

Den Nutzerinnen und Nutzern im Netz muss aber klar sein, dass die tatsächliche Kontrolle zur Selbstbestimmung über die eigenen personenbezogenen Informationen umso schwächer ausfällt, je mehr diese an die Anbieter „verkauft" werden. Nutzungsbestimmungen, die dieses außer Acht lassen, fördern daher nicht den Datenschutz, sondern unterlaufen tendenziell die informationelle Selbstbestimmung. Kommen biometrisch vermessbare Merkmale von Gesichtern zu den Profilbildungen hinzu, lassen sich inzwischen verschiedene Portraitfotos durch leistungsfähige Rechenzentren verblüffend präzise und schnell abgleichen. Einmal abgeglichen, ergeben die Ergebnisse zusätzliche Metadaten und inhaltliche Werte: Es entstehen aussagekräftige Zusammenhänge zwischen den Informationsinhalten zu Bild A und – im erfolgreichen Fall eines Abgleichs – den verknüpften Informationsinhalten zu Bild B, C und weiteren Bildern. Das Ergebnis ist eine kumulierende oder sogar eine potenzierende Informationsmenge. Es lassen sich damit sogar ganze Lebensläufe erstellen und damit Informationslücken schließen, die der Nutzer vielleicht bewusst nicht schließen wollte. Einmal im Netz erhoben und weiterverarbeitet, gibt es keine reale Chance mehr, Personenbezüge mit biometrischen Merkmalen sowie die zahlreichen Datenkorrelationen wieder wirksam aus dem Netz zu löschen.

Datenschutzbeauftragte: Nur mit Einwilligung der Betroffenen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat im März 2014 die Entschließung: „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!" verabschiedet. Wenngleich die Nutzung biometrischer Daten zunehmend an der Tagesordnung ist, wird jedoch häufig verkannt, dass Erzeugung biometrischer Templates in hohem Maße die schutzwürdigen Interessen Betroffener berührt. Daher hat die Konferenz in mehreren Punkten klargestellt, dass hierbei das informationelle Selbstbestimmungsrecht von Betroffenen in höchstmöglicher Weise berücksichtigt werden müsse:

- Die Erhebung, Verarbeitung und/oder Nutzung biometrischer Daten zur Gesichtserkennung zum Zweck der Erstellung eines dauerhaften biometrischen Templates kann nur bei Vorliegen einer wirksamen Einwilligung des Betroffenen im Sinne des § 4 a Bundesdatenschutzgesetz (BDSG) rechtmäßig erfolgen.
- Die Einwilligung in die Erstellung biometrischer Templates zur Gesichtserkennung muss aktiv und ausdrücklich durch den Betroffenen erteilt werden. Die Betroffenen müssen vor der Erteilung der Einwilligung über die Funktionsweise der Erstellung und Nutzung der sie möglicherweise betreffenden Templates und die damit verfolgten Zwecke und Risiken in klarer und verständlicher Weise umfassend informiert werden. Eine Zweckänderung ist unzulässig. Sie bedarf einer Einwilligung, die dem Standard an die Einwilligungen bei der Verarbeitung besonderer personenbezogener Daten gemäß § 4 a Absatz 3 BDSG entspricht.
- Die Einwilligung kann nicht durch den Verweis auf entsprechende Klauseln in allgemeinen Nutzungsbedingungen oder Datenschutzerklärungen ersetzt werden.
- Für eine logische Sekunde kann es nach § 28 Absatz 1 Satz 1 Nummer 2 beziehungsweise Nummer 3 BDSG auch ohne Einwilligung zulässig sein, ein Template zu erstellen, mit dem ein Abgleich mit bereits vorhandenen, zulässigerweise gespeicherten Templates im Rahmen des von der Einwilligung abgedeckten Zwecks möglich ist. Betroffene sind über den Umstand, dass Bilder zum Abgleich mit bestehenden Templates verwendet werden, zu informieren.
- Derartige biometrische Templates zum automatischen Abgleich, bei denen eine Einwilligung fehlt, sind unverzüglich nach dem Abgleich zu löschen.
- Die Speicherung von biometrischen Templates von Dritten, die – anders als die Nutzer von sozialen Medien – regelmäßig nicht einwilligen können, ist ausgeschlossen.



DSK-Entschließung „Biometrische Gesichtserkennung durch Internetdienste – Nur mit Wahrung des Selbstbestimmungsrechts Betroffener!" unter: www.lfd.niedersachsen.de > Allgemein > DSB-Konferenzen > Entschließungen

Datenschutzgerechtes Cloud Computing: Von der Kunst, Wolken transparent zu gestalten

Cloud Computing ist kein neues Thema, aber eines von hoher Aktualität und weiterhin zunehmender Bedeutung. Wurden früher noch Begriffsdefinitionen an den Anfang eines entsprechenden Artikels gestellt, hat sich die „Cloud" mittlerweile zum geflügelten Wort entwickelt. Nicht nur unter IT-Experten, sondern auch im alltäglichen Sprachgebrauch symbolisiert sie ein allgegenwärtiges Instrument arbeitsteiliger Datenverarbeitung, das von vielen genutzt, jedoch von den wenigsten durchschaut wird.

Bereits in meinem XXI. Tätigkeitsbericht (Seite 87) habe ich ausführlich hierzu Stellung genommen und auf die von der Konferenz der Datenschutzbeauftragten (DSK) zu dieser Thematik erhobenen Anforderungen hingewiesen. Die im September 2011 von den deutschen Datenschutzbehörden veröffentlichte Orientierungshilfe „Cloud Computing" gab erstmals umfassende Hilfestellungen, um die komplexen datenschutzrechtlichen Aspekte dieser Technologie zu identifizieren und eine angemessene Risikobewertung bezüglich der betroffenen Problemfelder zu ermöglichen. Die von allen Datenschutzbeauftragten des Bundes und der Länder getragene Publikation fand große Resonanz und wurde auch im Rahmen meiner Beratungstätigkeit erfolgreich unterstützend eingesetzt.

Aktualisierte Orientierungshilfe liegt vor

Orientierungshilfe Cloud Computing: www.lfd.niedersachsen.de > Technik und Organisation > Orientierungshilfen > Cloud Computing
Deeplink: http://www.lfd.niedersachsen.de/download/61457/Orientierungshilfe_Cloud-Computing_AK_Technik_AK_Medien_-_Stand_09. Oktober 2014_.pdf

Doch nichts ist so gut, dass es nicht noch verbessert werden könnte. Nicht nur die rasante technologische Entwicklung und die zunehmende Einsatzbreite von Cloud Computing machten ein Update der Orientierungshilfe notwendig. Auch die im Rahmen der NSA-Affäre gewachsenen Erkenntnisse um die besonderen datenschutzrechtlichen Risiken beim internationalen Datenverkehr (siehe auch Seite 113) waren Auslöser für Ergänzungen und Vertiefungen. Nach intensiver Vorarbeit verschiedener Arbeitsgruppen verabschiedete die 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2014 die neue Version 2.0 der Orientierungshilfe „Cloud Computing". Wesentliche Neuerungen sind

- die Notwendigkeit der für alle Beteiligten transparenten Gestaltung von Auftrags- und Unterauftragsverhältnissen,
- die Verpflichtung der Cloud-Anbieter zur Benennung aller Standorte, an denen personenbezogene Daten verarbeitet werden,
- die speziellen Anforderungen beim grenzüberschreitenden Datenverkehr, insbesondere außerhalb der EU und des Europäischen Wirtschaftsraumes (EWR) und
- die im Rahmen der technisch-organisatorischen Betrachtung neu hinzugekommenen speziell datenschutzrechtlichen Schutzziele der Datensparsamkeit, der Intervenierbarkeit und der Nicht-Verkettbarkeit.

Auch Anbieter zeigen Verantwortung

Im Auftrag der Arbeitsgemeinschaft der Leiter der Datenzentralen der Bundesländer (ALD) erarbeiteten der Landesbetrieb Daten und Information Rheinland-Pfalz (LDI) und die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH den Entwurf einer Richtlinienempfehlung für die Ausschreibung, die Vergabe und den Betrieb von öffentlichen Aufträgen in der Cloud mit dem Titel „Cloud-Services der Datenzentralen“. Die Version 3.0 des Richtlinienentwurfes wurde sowohl vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch vom Arbeitskreis Technische und organisatorische Datenschutzfragen (AK Technik) der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begleitet. Nach Aufnahme verschiedener Empfehlungen und Hinweise kam der AK Technik zu dem Ergebnis, dass der Entwurf der Richtlinienempfehlung „zweckmäßige Wege zur Realisierung von datenschutzkonformen Cloud-Dienstleistungen“ aufzeige. Zudem wurde der Ansatz begrüßt, „personenbezogene Daten nur in solchen Cloud-Strukturen zu verarbeiten, die in nationalen zertifizierten Hochsicherheitszentren betrieben werden und somit den Datenschutzregeln der Europäischen Union unterliegen“.

Entwurf einer bundesweiten Richtlinienempfehlung: „Cloud-Services der Datenzentralen“ (Version 3.0, Stand 3. Juni 2014)

Ich halte dies für ein gelungenes Beispiel umfassender Kooperation, die es ermöglicht, das Thema Datenschutz nicht nur beim Betrieb, sondern auch schon im Vorfeld bei Ausschreibung und Vergabe einer projektierten Datenverarbeitung zielführend zu positionieren.

Noch ein Vertrauensverlust: Der Heartbleed-Bug – Sicherheitslücke im Sicherheitsprotokoll

Das Bayerische Landesamt für Datenschutzaufsicht (LDA) führte im Herbst 2014 eine umfangreiche Prüfung von Servern auf Vorliegen des so genannten Heartbleed-Bug durch. Die im Rahmen der Erhebung ermittelten Server in Niedersachsen wurden meiner Behörde mitgeteilt. Die benannten Sicherheitslücken konnte ich durch eigene Prüfung bestätigen.

Heartbleed ist eine Sicherheitslücke in einer Implementierung des TLS-Protokolls (Transport Layer Security), dem Nachfolge-Kommunikationsprotokoll von Secure Socket Layer (SSL), das eine Verschlüsselung beinhaltet und deshalb insbesondere für den vertraulichen Transport von E-Mails und im Browserverkehr (vergleichbar mit https) eingesetzt wird. Betroffen ist nicht das Konzept des Protokolls selbst, sondern die im Open-Source-Bereich weitverbreitete Implementierung OpenSSL. Die Sicherheitslücke basiert darauf, dass der Server die Länge der übermittelten Daten nicht prüft, sondern den Absenderangaben vertraut. Dies führt dazu, dass ein Angreifer bis zu 64 Kilobyte aus dem Speicher des angegriffenen Servers auslesen kann. Diese können beliebige Daten, insbesondere auch personenbezogene Daten Dritter enthalten, die vor dem Angreifer mit dem Server kommuniziert haben. Damit ermöglicht diese Sicherheitslücke gleichzeitig eine Datenschutzverletzung.
Ursache sind erhebliche Mängel im schwierig zu pflegenden Programmcode von OpenSSL. Inzwischen hat es nicht nur Anstrengungen gegeben, die Fehler zu beseitigen, sondern auch, den Programmcode von OpenSSL insgesamt zu bereinigen. Mitarbeiter des OpenBSD-Projektes (OpenBSD ist ein frei verfügbares, quelloffenes Derivat des Unix-Betriebssystems) haben zudem eine Abspaltung namens LibreSSL veröffentlicht, die sich zum Ziel gesetzt hat, durch Verschlanken des Programmcodes die Fehleranfälligkeit grundsätzlich zu verringern. Des Weiteren hat die Firma Google inzwischen mit BoringSSL einen eigenen weiteren Ableger von OpenSSL entwickelt.

Open Source ermöglicht schnelle Fehlerkorrektur

Die Heartbleed-Lücke macht deutlich, dass die Fehleranfälligkeit eines Programmes weniger vom Entwicklungsmodell (frei verfügbar und quelloffen oder kommerziell und geschlossen) abhängt, als vielmehr von der Übersichtlichkeit des Programmcodes und der Zahl und Arbeitssorgfalt derer, die diesen auch tatsächlich prüfen. Gleichzeitig zeigt der Prozess um die Bereinigung der entdeckten Lücken die Vorzüge des Open-Source-Modells: Als Serverbetreiber ist man nicht dem Hersteller ausgeliefert und muss nicht warten, bis dieser, eventuell mit

erheblicher zeitlicher Verzögerung, Sicherheitsaktualisierungen bereitstellt, sondern man kann auch selbst die Fehlerkorrektur in Angriff nehmen oder einen Dritten damit beauftragen. Hier zeigt sich exemplarisch eine weitere typische Vorgehensweise im Open-Source-Bereich: Für wichtige Funktionen gibt es in aller Regel verschiedene Lösungsansätze, die von unterschiedlichen Teams entwickelt werden. So kann sich durch Konkurrenz die bessere Lösung durchsetzen, oder es können sich für ähnliche aber im Detail unterschiedliche Probleme angepasste Lösungen entwickeln. Hinzu kommt, dass der Anwender auf mehrere Lösungen zugreifen und im Falle kritischer Fehler auf eine Alternative ausweichen kann.

Unternehmen reagieren zu langsam

Bei der Überprüfung der Server fand das LDA auf bayerischen Mailservern die erschreckend hohe Zahl von 44 Unternehmen, welche die Heartbleed-Sicherheitslücke immer noch nicht geschlossen hatten, obwohl zu dem Zeitpunkt bereits seit einem halben Jahr in den Medien darüber berichtet worden war. Über die von der Heartbleed-Lücke betroffenen Server außerhalb Bayerns verständigte das LDA die jeweils örtlich zuständigen Datenschutzbehörden. Meine aufgrund der sehr beschränkten technischen Sachmittel unter erschwerten Bedingungen durchgeführten Überprüfungen ergaben, dass von dreißig gemeldeten Servern zum Zeitpunkt der Nachprüfung neun Server nach wie vor angreifbar waren, obwohl bereits seit einigen Tagen über die Sicherheitslücke prominent in den Medien berichtet worden war und eine aktualisierte Fassung von OpenSSL bereitstand.

Einrichtung eines Prüflabors geplant

Ich beabsichtige, in den Folgejahren ab 2015 ein Prüflabor in meinem Technikreferat zu konzipieren, einzurichten und zu betreiben, mit dessen Möglichkeiten Standardplattformen, Anwendungen und Apps für verschiedene Endgeräteklassen in ausgesuchten Prüffällen durch Informatiker mit dem Fokus auf technisch-organisatorische Schutzmaßnahmen getestet und untersucht werden können. Damit wäre in Zukunft die Option gegeben, technische Unzulänglichkeiten nachweisbar zu dokumentieren und in der Aufsichts- und Beratungspraxis die Faktenlage wirksamer für Hinweise, Anordnungen oder Beanstandungen heranziehen zu können.

Weitere Informationen:

Tätigkeitsbericht des Bayerischen LDA vom 23. März 2015 und Pressemitteilung dazu unter https://www.lda.bayern.de/lda/datenschutzaufsicht/lda _ daten/dsa _ Taetigkeitsbericht2014.pdf und http://www.lda.bayern.de/lda/datenschutzaufsicht/p _ archiv/2015/pm003.html

Bundesgerichtshof zu Online-Bewertungen: Ärzte müssen Netzöffentlichkeit dulden

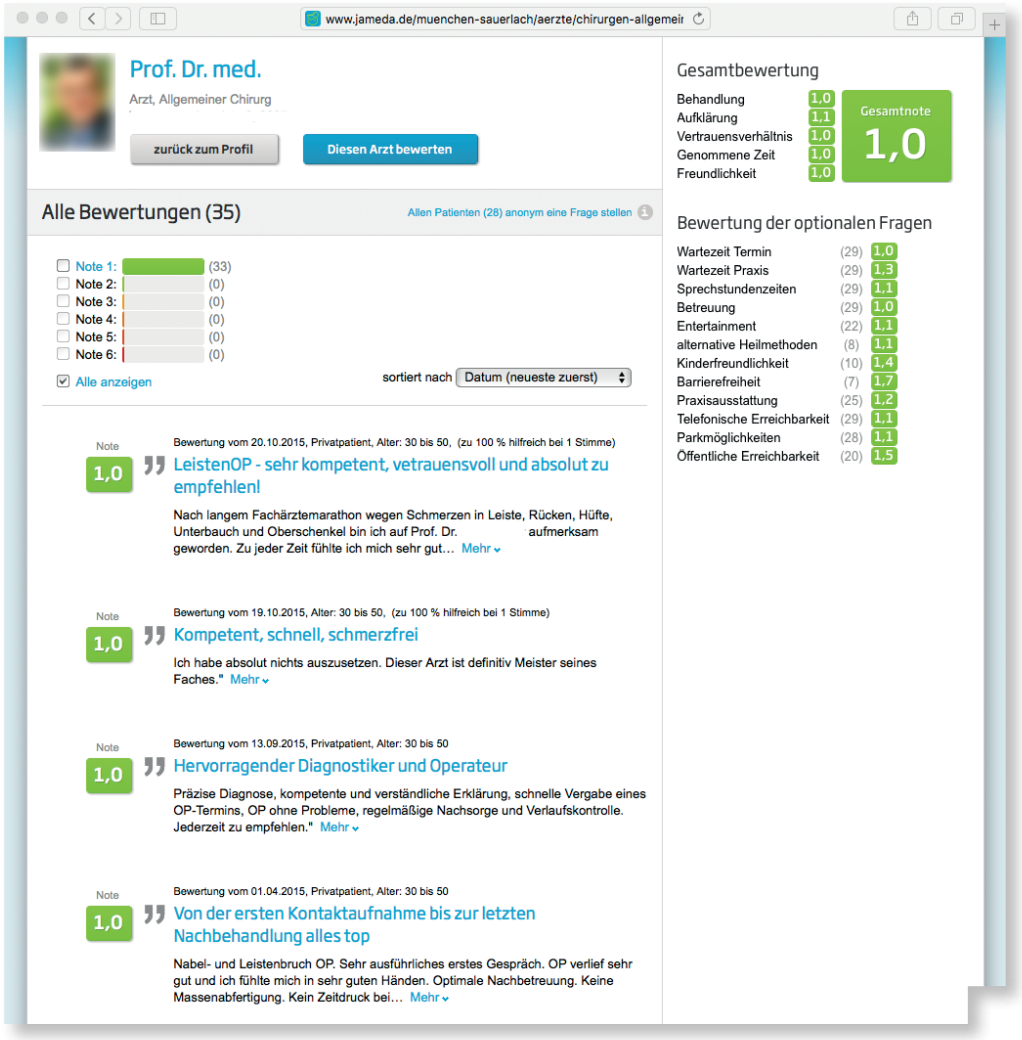
Ein wichtiges Urteil mit grundlegender Bedeutung für meine Aufsichtsaufgaben hat am 23. September 2014 der Bundesgerichtshof (BGH) gefällt. Es ging um die Frage der Zulässigkeit der Erhebung, Speicherung und Übermittlung von personenbezogenen Daten im Rahmen eines Such- und Bewertungsportals über Ärzte im Internet. Ein Arzt hatte die Löschung aller ihn betreffenden Einträge auf dem Portal www.jameda.de verlangt. Der BGH sah jedoch die Privatsphäre des Arztes nicht als tangiert an und wies die Klage zurück[1].

Der BGH beschäftigte sich mit der Frage, ob es ein Arzt grundsätzlich dulden muss, dass seine Leistung im Internet bewertet wird. Hierzu zog er ausschließlich die Vorschriften des Bundesdatenschutzgesetzes (BDSG) zur Prüfung heran und wies zunächst darauf hin, dass das so genannte Medienprivileg (§ 57 Abs. 1 Satz 1 Rundfunkstaatsvertrag, § 41 Abs. 1 BDSG) für Bewertungsportale nicht gelte, solange keine journalistisch-redaktionelle Bearbeitung stattfinde.
Die Revision gegen das Urteil der Vorinstanz vom 19. Juli 2013 wurde zurückgewiesen. Der BGH bestätigte damit ein Urteil des Landgerichts München (Az.: BGH VI ZR 358/13). Dem Kläger stehe weder ein Anspruch auf Löschung noch auf Unterlassung der Veröffentlichung der streitgegenständlichen Daten zu, so die Richter. Die Interessen des Klägers am Ausschluss der Erhebung, Speicherung oder Veränderung der Daten überwögen die Interessen der Beklagten und der Nutzer nicht. Den schutzwürdigen Interessen des Klägers werde durch die Kontrollmechanismen der Beklagten hinreichend Rechnung getragen. Nach dem Wortlaut des § 29 Abs. 2 Satz 1 BDSG ist die Übermittlung personenbezogener Daten zulässig, wenn der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

Öffentliches Interesse überwiegt

In Bezug auf Bewertungsportale im Internet ist die Vorschrift nach der Rechtsprechung des BGH-Senats verfassungskonform dahingehend auszulegen, dass die Zulässigkeit der Übermittlung der Daten an die abfragenden Nutzer aufgrund einer Gesamtabwä-

1 Urteil des Bundesgerichtshofs (BGH), VI ZR 358/13 vom 23. September 2014, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=f52175775bb16956b601caa5197a6d03&nr=69297&pos=0&anz=1;
BGH, Mitteilung der Pressestelle, Nr. 132/2014 vom 23.9.2014 zum Urteil vom 23. September 2014 – VI ZR 358/13: „Bundesgerichtshof lehnt den Anspruch eines Arztes auf Löschung seiner Daten aus einem Ärztebewertungsportal ab“, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&nr=68915&linked=pm;
Bundesgerichtshof, Mitteilung der Pressestelle Nr. 130/2014, Terminankündigung mit in Frage stehenden Rechtsgrundlagen und Sachverhaltsdarstellung, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=1d3d520c8804ae6b64d136103413194e&anz=1&pos=0&nr=68878&linked=pm&Blank=1.



gung zwischen dem Persönlichkeitsrecht des Betroffenen und dem Informationsinteresse desjenigen, dem die Daten über das Internet übermittelt werden, beurteilt werden muss. Dabei sind die schutzwürdigen Interessen des Betroffenen den Interessen des Abrufenden an der Kenntnis der Daten und desjenigen, der die Daten übermittelt, an deren Weitergabe gegenüberzustellen. Der vom Wortlaut der Vorschrift verlangten glaubhaften einzelfallbezogenen Darlegung des berechtigten Interesses am Abruf bedarf es hingegen nicht.

Im vorliegenden Fall sei der Bereich der „Sozialsphäre" betroffen, so der BGH. Dieser würde lediglich das berufliche Wirken des Arztes betreffen, und damit stünde der Arzt im freien Wettbewerb. Auf der anderen Interessenseite sei das öffentliche Interesse an Bewertungsseiten im Internet zu bewerten, das in diesem Fall höher wiege. Erfolgreich wehren könnte sich der Arzt lediglich gegen unwahre Tatsachenbehauptungen oder stigmatisierende Äußerungen. Im vorliegenden Fall sei dies jedoch nicht zutreffend gewesen.

Smart-TV, Streaming, Mediatheken, Rückkanal:

Auch wenn ich wie meine Kolleginnen und Kollegen in den anderen Bundesländern nicht für die Datenschutzaufsicht über den öffentlich-rechtlichen Rundfunk zuständig bin, ist die Fortentwicklung der technischen Basis der Fernsehtechnik datenschutzrechtlich bedeutsam für Millionen niedersächsischer Zuschauer. Meine Behörde hat das Thema deshalb im Berichtszeitraum in bundesweiten Arbeitsgruppen begleitet. Vorrangig geht es um die Weiterentwicklung der Flachbildfernseher zu einem internetfähigen Smart-TV sowie das zunehmende Informationsangebot der Mediatheken und Streamingdienste, insbesondere aber um die Einführung von Rückkanälen, die den Zuschauer identifizierbar machen[1].

Während sich die Digitalisierung der Fernsehtechnik seit der Einführung des Videotextes vor allem innerhalb des Gerätes vollzog, woran sich auch mit dem Aufkommen der Flachbildfernseher zunächst nichts änderte, folgte im nächsten Schritt die Umstellung von analoger auf digitale Ausstrahlung, zunächst im terrestrischen Bereich, anschließend aber auch über Satellit und Kabel. Fast zeitgleich mit dem Aufkommen des hochauflösenden Fernsehens wandelte sich der Fernseher jedoch vom reinen Empfangsgerät zum Wohnzimmercomputer, der nicht nur Filme und Bilder von USB-Geräten und Kameraspeicherkarten wiedergibt, sondern der über ein lokales Netzwerk (LAN) oder ein drahtloses lokales Netzwerk (WLAN) auf den PC im Hause, aber vor allem auf das Internet zugreifen und damit auch Daten ins Internet übermitteln kann.

Fernsehgeräte sind angreifbar wie Smartphones

Damit unterlag das Fernsehgerät einem ähnlichen Wandel wie dies beim Telefon mit der Entwicklung zum Mobiltelefon und weiter zum Smartphone der Fall war. So hat sich der „Fernsehapparat" zum Smart-TV weiterentwickelt. Ein wesentliches Merkmal eines Smart-TV stellt neben der herkömmlichen Fernsehfunktion die Tatsache dar, dass verschiedene Applikationen mit Zusatzfunktionen zur Verfügung stehen, wie sie auch bei Smartphones zur Anwendung kommen. Zusätzlich sind insbesondere die Internet-Fähigkeiten sowie Hybrid Broadcast Broadband TV (HbbTV) verfügbar. HbbTV bietet beispielsweise Informationen zum laufenden Programm oder Zugang zu weiteren Inhalten aus der Mediathek. Voraussichtlich werden bis 2016 in Deutschland über ein Drittel aller Haushalte einen HbbTV-fähigen Fernseher nutzen[2].
Das Fernsehgerät ist in der Summe all dieser Eigenschaften heute bereits häufig ein vollwertiger Rechner, der vielfach auf Komponenten aus dem Bereich der Smartphones basiert und auch deren Betriebssysteme nutzt, überwiegend Android des Unternehmens Google. Mit der Etablierung dieses Betriebssystems können dieselben Risiken für die Privatsphäre und die IT-Sicherheit auftreten, wie dies bei Smartphones bereits bekannt ist. Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Die Erweiterung um die Rückkanalfähigkeit über die Netzwerkverbindung des Smart-TV bringt allerdings auch die Möglichkeit zur

1 In Niedersachsen gibt es derzeit 17 TV-Sender, die von der Niedersächsischen Landemedienanstalt lizenziert sind. Eine aktuelle Übersicht, ob hier Mediathek- und Rückkanal-Angebote existieren, ist mir derzeit nicht bekannt.

2 Vergl. Forschungsergebnisse des Center for Advanced Security Research Darmstadt (CASED): „Smarte Spione – Fernsehsender analysieren SmartTV-Besitzer", 15. Mai 2013, http://www.tu-darmstadt.de/vorbeischauen/aktuell/archiv_2/2013_1/einzelansicht_69632.de.jsp, http://www.mainpost.de/ueberregional/politik/zeitgeschehen/Wenn-der-Fernseher-zum-Spion-wird;art16698,7828363

Anonymer Medienkonsum zunehmend gefährdet

Übermittlung von Daten der Nutzer mit sich. Nicht immer ist das den Nutzern klar, und nicht immer entspricht diese Funktion der bewussten Absicht der Nutzer.
Während die Nutzer beim gewöhnlichen Fernsehen anonym bleiben, so sind sie jetzt unter Umständen identifizierbar. Beispielsweise können Informationen über Nutzungsverhalten oder Inhalte angeschlossener USB-Laufwerke an den Hersteller und den Inhalteanbieter übermittelt werden. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es sich handelt. Insgesamt fehlt es also häufig an der notwendigen Transparenz über die Abläufe und die Datenerhebungen und -übermittlungen .
Auch wenn zumindest gegenwärtig ein Betrieb noch ohne Internetanbindung möglich ist, verweisen die Fernsehgerätehersteller bereits auf die Möglichkeit, die im Gerät vorhandenen Programme über das Internet zu aktualisieren. Kaum eine Nachrichtensendung verzichtet auf Hinweise zu weiterführenden Informationen im Internet, die man dann zweckmäßigerweise gleich am Fernsehgerät abruft.

Grundsatz der Möglichkeit zur anonymen Information

Für das demokratische System unserer Gesellschaft ist eine wesentliche Voraussetzung zur politischen Teilhabe, sich unbeobachtet aus frei zugänglichen Quellen, vor allem aus Rundfunk und Fernsehen sowie der Presse, informieren zu können. Sobald dies nicht mehr möglich ist, besteht die Gefahr, dass Bürger aus Angst vor Beobachtung und eventuellen Nachteilen darauf verzichten, bestimmte Quellen zur Information zu nutzen, und dass damit bestimmte Ansichten und Veröffentlichungen faktisch von der öffentlichen Diskussion ausgegrenzt werden. Aus diesem Grunde haben die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, der so genannte Düsseldorfer Kreis, und die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten im Mai 2014 ein gemeinsames Positionspapier[3] zum Thema Smart-TV („Smartes Fernsehen nur mit smartem Datenschutz“) veröffentlicht, in dem der Erhalt der Möglichkeit zur anonymen Nutzung auch von Smart-TV-Inhalten und die folgenden datenschutzrechtlichen Aspekte gefordert werden[4]:

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.
2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:
   - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.
   - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.

3 Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten „Smartes Fernsehen nur mit smartem Datenschutz“, Stand: Mai 2014, https://www.datenschutz.hessen.de/ft-fernrund.htm#entry4208
4 vergl. http://www.zdf.de/ZDF/zdfportal/blob/26583636/1/data.pdf

- Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat.
- Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z. B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.
- Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „Privacy by Default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommunikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, so zum Beispiel die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.
4. Smart-TV-Geräte, die HbbTV- Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen.

Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

Nutzer müssen informiert und aktiv einwilligen

In diesem Positionspapier stellen die Datenschutzbeauftragten fest, dass Web- und HbbTV-Dienste dem Telemediengesetz unterfallen und daher bei Verarbeitung personenbezogener Daten insbesondere die Anforderung der informierten aktiven Einwilligung (Opt-In) zu beachten sei. In der Vergangenheit haben die Geräte mitunter bereits beim Einschalten und unmittelbar nach jedem Programmwechsel eine Internetverbindung unter anderem zum Gerätehersteller, aber auch zu den Programmanbietern aufgebaut. Die ARD hat hier inzwischen vorbildlich reagiert: Beim Aufruf der ARD-Programme mit einem HbbTV-fähigen Empfangsgerät erhält der Nutzer oder die Nutzerin zu Beginn einen entsprechenden Hinweis auf dem Bildschirm mit der Möglichkeit, die Datenschutzerklärung einzusehen. Diese wird zusammen mit dem Fernsehsignal ausgestrahlt, so dass der Betroffene entsprechend informiert wird, bevor die Internetverbindung aufgebaut wird und erste personenbezogene Daten fließen.
Die Forderung nach der informierten Einwilligung gilt insbesondere auch für Daten, die vom Fernsehgerät an dessen Hersteller gesendet werden, was zumindest in der Vergangenheit ohne Kenntnis der Nutzer erfolgte. Diese Forderungen sind im Übrigen nicht neu, sondern werden von den Datenschutzaufsichtsbehörden auch international bereits seit Jahren, seit Einführung des IP-basierten Fernsehens, also auf Grundlage der Internetübertragungsprotokolle, erhoben. Hier erwarte ich, dass sich datenschutzgerechte Lösungen durchsetzen und für ähnliche aber im Detail unterschiedliche Probleme angepasste datenschutzrechtskonforme und -freundliche Lösungen entwickelt werden. Das hätte die Wirkung, dass die Anwender auf mehrere Lösungen zugreifen und im Falle kritischer Fehler auf eine Alternative ausweichen könnten.

10.2 Spezifische Handlungsfelder in der Landesverwaltung

Informationssicherheit in Behörden und Kommunen gefährdet: Strategische Neupositionierung dringend erforderlich

Die aus der weltweiten Kommunikationsüberwachung (siehe hierzu auch meinen Beitrag „Globale Überwachung durch Geheimdienste“, Seite 12) abgeleiteten Forderungen an Regierungen und Parlamente wurden öffentlich gemacht. Jetzt gilt es, strategische Vorkehrungen zu treffen, um Technik und Prozesse aller öffentlichen Aufgabenwahrnehmungen bei Bund, Ländern und Kommunen wirksamer gegen Verluste der Integrität und Vertraulichkeit zu schützen. Die öffentlichen Stellen in Niedersachsen wurden auch im Berichtszeitraum von meiner Behörde beraten und vor den wachsenden drohenden Gefahren gewarnt. Sie sollten jetzt umgehend strategisch und operativ handeln.

Niemanden kann die Tatsache ernsthaft überraschen, dass es technisch möglich war und ist, Telekommunikationsinfrastruktur abzuhören und auch andere Angriffsvektoren zu nutzen, um aktive Netzkomponenten, Server und Endgeräte sowie beliebige mobile IT-Systeme mit verschiedenen Angriffsstrategien und dem Zweck globaler Spionage zu kompromittieren. Derartige Risikobetrachtungen und Gefahreneinschätzungen sind in meiner Behörde seit vielen Jahren nahezu tagtäglich Gegenstand datenschutzrechtlicher Beratung und Prüfung. Überraschend waren in den letzten beiden Jahren allerdings das Ausmaß und der flächendeckende Charakter der Massenspionage.

Die wichtigsten Programme von NSA (National Security Agency; US Nachrichtendienst) und des GCHQ (Government Communications Headquarter; Britischer Geheimdienst) sind jedes für sich mächtige Werkzeuge:

- PRISM (Datenerhebung von Kommunikationsverbindungen, Datenerfassungen von Webseiten der großen US-Anbieter wie Microsoft, Yahoo, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple)
- Boundless Informant (Analyse der von der NSA erhobenen Datenmengen aus einer Fülle von E-Mails und Telefonmetadaten mittels Data Mining und künstlicher Intelligenz; geografische Visualisierung der Daten)
- Tempora (Programm des GCHQ: schöpft Online- und Telefonkommunikation im globalen Maßstab ab, insbesondere Internetknotenpunkte und das transatlantische Glasfasernetz von und nach UK)
- XKeyscore (Zusammenfassung von Metadaten, E-Mails und Chats einer Zielperson)
- MICT (Mail Isolation Control and Tracking; Metadatenerfassung durch fotografierte Postbriefe)
- FAIRVIEW (NSA-Programm zur Erhebung großer Datenmengen außerhalb des US-Hoheitsgebietes mittels US-Telekommunikationsunternehmen und deren Kontakten zu ausländischen Unternehmen)
- Genie (Botnet unter der Kontrolle der NSA, um befallene Rechner fernzusteuern und mittels XKeyscore zu analysieren)
- Bullrun (liest verschlüsselte Daten über zahlreiche Angriffswege im Internet mit; z. B. können Zertifizierungsstellen oder Zufallszahlengeneratoren mit Schwachstellen infiltriert werden, um diese später leicht knacken zu können)
- Edgehill (zur Gewinnung von verschlüsselten Daten des GCHQ, ähnlich Bullrun)
- CO-TRAVELER Analytics (Erhebung von Standortinformationen mehrerer hundert Millionen Mobilfunkanschlüsse täglich und Erstellung umfassender Bewegungs- und Beziehungsprofile)
- Squeaky Dolphin (NSA-Programm zur Verfolgung und Analyse von Nutzerinteraktionen in Social Networks wie Facebook, YouTube und Blogger.com in Echtzeit)
- ICREACH (zentrale Suchmaschine der NSA für die verschiedenen Datenbanken der US-Nachrichtendienst-Community)

Keylogger, Backdoors, Trojaner

Neben den von Nachrichtendiensten genutzten Programmen wie PRISM, Tempora oder XKeyscore (siehe Info-Kasten) finden jedoch auch operativ gezielt steuerbare Methoden Anwendung, wie sie etwa auch bei der Quellen-Telekommunikation (Quellen-TKÜ[1]) bekannt wurden. Es sind dies die Ausnutzung bekannter Sicherheitslücken (so genannter Exploits), das Programmieren eigener Trojaner oder von Aufzeichnungsprogrammen für Tastaturanschläge („Keylogger") und anderer kompromittierender Spionageprogramme, die als Sortiment von Angriffswerkzeugen nicht nur in der Hackerszene und bei Computerkriminalitätsdelikten mit meist finanziell moti-

1 Vgl. meinen XIX. Tätigkeitsbericht 2007–2008, Seite 38, Kapitel „Ein neues Grundrecht ... und die Notwendigkeit, Gesetze nachzubessern" zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", Urteil des BVerfG zum „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" (BVerfG, 1 BvR 370/07 vom 27. Februar 2008, Absatz-Nr. 1–333, http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html) und den Konsequenzen zur Quellen-TKÜ

vierten Angriffen bekannt sind. Daneben gibt es für Nachrichtendienste in manchen Ländern die Möglichkeit, Hersteller von Hardware (z. B. Microcomputer, Rechnerkomponenten, Router) oder von Software (z. B. Firmware, Betriebssysteme, Netzwerksoftware, Middleware, Sicherheitssoftware, Verschlüsselungssoftware zur Implementierung von Hintertüren, so genannte Backdoors) zum gezielten Ausleiten von Daten zu bewegen oder sogar durch nationale Regelungen gesetzlich zu verpflichten. Als Begründung für nachrichtendienstliche Informationsbeschaffung diente bislang stets die Terrorismusbekämpfung. Inzwischen mehren sich Hinweise, dass es auch um politische und wirtschaftliche Vorteile bei Verhandlungspositionen geht.

Neubewertung der IT-Architektur ist zwingend

Die Entschließungen der Konferenz der Datenschutzbeauftragten von Bund und Ländern (DSK) und die damit verbundenen Forderungen an die Regierungen und Parlamente nach wirksamen politischen und gesetzgeberischen Maßnahmen zum Schutz von Informationssicherheit und personenbezogenen Daten im Rahmen des Grundrechtsschutzes sind zweifellos wichtig. Ebenso wichtig ist es jedoch, sich den IT-Aufgaben einschließlich der strategischen Planungen und der technischen Implementierungen zu widmen. Es gilt, weitere strategische und operative Vorkehrungen zu konzipieren, um die Informationstechnik, die Netzinfrastruktur und die Prozesse aller öffentlichen Aufgabenwahrnehmungen bei Bund, Ländern und Kommunen wirksamer gegen Verluste der Integrität und Vertraulichkeit zu schützen. Auch die kooperativen Ansätze bei Datenübermittlungen, Mitnutzung von IT-Verfahren anderer öffentlicher Stellen oder gemeinsamen Verfahren zwischen den Behörden und föderalen Ebenen müssen unter diesen Aspekten neu bewertet werden.
Das setzt eine grundsätzliche und zugleich kritische Bestandsaufnahme der IT und ihrer Prozesse voraus. Ich halte daher mindestens folgende Schritte für erforderlich:

1. **Verbindungen zum Internet nur kontrolliert zulassen**
   Wenn sich die Erkenntnis durchsetzt, dass zentrale Hard- und Softwarekomponenten, die über das Internet von außen erreichbar sind, von den beschriebenen Angriffsszenarien betroffen sein können, liegt es nahe, diese Mechanismen der ständigen Erreichbarkeit durch neue und wirksamere, abschirmende, filternde und analytische Schutzmaßnahmen zu ersetzen. Es bedarf der systematischen Bewertung, welche der herkömmlichen Technologien tatsächlich welche Wirkung erzielen können, aber auch, was sie explizit nicht an Schutz zu leisten vermögen.
2. **Virtualisierungstechniken konsequenter nutzen**
   Die Virtualisierung von Datenverarbeitungsprozessen, insbesondere denjenigen, die regelmäßig eine Verbindung zum Internet benötigen, muss als bewährte Methode zur Standardarchitektur für Browserclients und den E-Mail-Verkehr implementiert werden. Der Browser gilt als häufigstes Einfallstor für Malware und aktive Inhalte, besonders seit es interaktive Funktionen des Web 2.0 gibt. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat bereits 2011 Empfehlungen veröffentlicht, sicheres Surfen durch den Betrieb des Browsers in einer virtuellen Maschine (Virtual Machine) zu betreiben. Dies vermindert deutlich die Gefahr, dass Angreifer aus dem Internet auf Daten des Hauptanwenders zugreifen können, da solche Versuche ins Leere geleitet werden können. Welche Virtualisierungstechniken im Einzelnen sinnvoll erscheinen, muss individuell sorgfältig abgewogen werden.
3. **Vertraulichkeitskriterien für Hersteller und Produkte festlegen**
   Die Frage, ob Hardware- und Softwareprodukte tatsächlich nur die Funktionen ausführen, die der gesetzlichen Aufgabe und den Vorgaben der für die Datenverarbeitung verantwortlichen Stelle (im Sinne des § 3 Abs. 3 NDSG oder § 3 Abs. 7 BDSG) entsprechen, muss sorgfältiger geprüft werden. Mir sind keine allgemeingültigen Vertraulichkeitskriterien bekannt, nach denen

Hersteller und Produkte geprüft worden wären. Vereinzelt dürfte es zu Anforderungen im Hochsicherheitsbereich kommen, jedoch wird bereits das Standardsicherheitsniveau verfehlt, wenn die Kontrolle darüber beim Hersteller liegt und nicht durch den Kunden beeinflussbar ist. Die Erhebung überschießender Daten sowie unbeabsichtigte oder unzulässige Datenverknüpfungen oder Datenübermittlungen müssen unterbunden werden, auch wenn diese Funktionen durch ein Standardprodukt vorgegeben werden. Das betrifft auch und besonders Standardbetriebssysteme (Windows, iOS, Android), Browserfunktionen, Standard-Office-Anwendungen, Netzkomponenten (z. B. Router und Middleware), aber ebenso Datenbankmanagementsysteme, Administrationswerkzeuge sowie bei Tablets und Smartphones[2] die ungehärteten Systeme in Kombination mit zahlreichen weiteren Anwendungsfunktionen (Telefonie, Videokonferenz, Officefunktionen, Social Media, unterschiedlichste Gerätesensoren, GPS-Ortung und -Geolokalisierung sowie Tracking etc.), sofern deren Grundfunktionen nicht dem Prinzip des Privacy-by-Design folgen.

Die Tatsache, dass ein Produkt einen hohen Marktanteil aufweist, befreit die verantwortliche Stelle nicht von der Sorgfaltspflicht, die Funktionen des Produktes auf unzulässige Datenverarbeitungen zu untersuchen. Die Leistungsbeschreibungen bei Ausschreibungen und die Zuschlagserteilung an Hersteller müssen ebenfalls die Frage einbeziehen, ob ein Hersteller aus einem EU-Mitgliedsstaat oder dem EWR stammt oder durch Sitz in einem unsicheren Drittland außerhalb der EU[3] dem Risiko der dort verpflichtenden Herausgabe von Kundendaten an Behörden und Regierungen unterworfen ist.

4. **Hard- und Softwarehersteller zur Fehlerbehebung verpflichten**

   Lizenz- und Supportverträge, die einem weltweit gebräuchlichen Standardtext folgen und dem Lizenz- und Supportkunden (hier: Behörde oder andere öffentliche Stelle) keine Mindestrechte zur Gewährleistung oder Reaktion auf Produktfehler einräumen, sind als einseitig verpflichtende Verträge abzulehnen. Solche Verträge haben Marktführer nicht selten „im Angebot", abweichende Vorstellungen des Kunden finden angesichts der Marktmacht des Anbieters keine Durchsetzung. Diese Verträge verstoßen jedoch nicht nur gegen das Wirtschaftlichkeitsgebot bei öffentlichen Haushalten, sondern verletzen auch die Schutzpflichten der verantwortlichen Stelle gegenüber den datenschutzrechtlichen Betroffenenrechten. Als Auftragnehmer trifft die verantwortliche Stelle die Pflicht, Auftragnehmer und die Produkte in der Funktion rechtskonform und effektiv zu steuern. Darauf muss auch bei Standardrahmenverträgen, Lizenz-Select-Verträgen, Standard-Supportverträgen und ähnlichen Vertragsmodellen geachtet werden. Treten Softwareschwachstellen und -lücken, Fehlimplementierungen oder veraltete oder als unsicher geltende Funktionen auf, muss der Hersteller vertraglich verpflichtet werden, innerhalb einer angemessenen Frist die Fehlerbeseitigung (Patch, Update, Upgrade) oder die Erarbeitung einer Alternativlösung zuzusichern und bereitzustellen. Meine Überprüfung im März 2014 der geltenden Lizenzrahmenverträge mit Microsoft vom 1. März 2011 beispielsweise, die mit dem Bundesverwaltungsamt abgeschlossen worden waren, ergaben eben solche Einschränkungen für die niedersächsische Landesverwaltung.

5. **Mit Open-Source-Strategie Wettbewerb datenschutzfreundlicher IT-Produkte beflügeln**

   In den meisten Fällen, in denen öffentliche Stellen Betriebssysteme und Office-Produkte einsetzen wollen, verschreiben sie sich den Produktlinien der Firma Microsoft. Die Windows-Betriebssysteme (aktuell 8.1, ab 2015 Windows 10 ohne Fortsetzung der bisherigen gestuften Versionsnum-

2 Vgl. gesonderter Beitrag „Einsatz mobiler IT-Endgeräte" Seite 128

3 Gem. Erwägungsgrund Nr. 57 Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:31995L0046&from=DE) ist die Übermittlung personenbezogener Daten in ein Drittland zu untersagen, wenn dieses kein angemessenes Schutzniveau bietet. Vgl. § 14 NDSG (Übermittlung an Personen oder Stellen in Staaten außerhalb des Europäischen Wirtschaftsraums) und §§ 4 b, 4 c BDSG

mern-Erhöhung), der Browser Internet Explorer und die Bürosoftware-Suite MS Office sind die in Behörden, aber auch in der gewerblichen Wirtschaft sowie bei Heimanwendern etablierten Standard-Softwareumgebungen. Damit treten leicht wirtschaftliche „Lock-in-Effekte" ein, eine Abhängigkeit, die Produkt- und Strategieeinengungen nach sich zieht und damit die Flexibilität für Informationssicherheit und technisch-organisatorische Datenschutzmaßnahmen schmälert.
Dennoch setzt sich in Behörden nur sehr langsam die Strategie durch, auf quelloffene Software umzusteigen und beispielsweise die Betriebssysteme durch LINUX-Derivate und die Bürosoftware-Suiten etwa durch LibreOffice oder OpenOffice zu ersetzen. Mit etwa 12.000 Arbeitsplätzen ist dies auf der Basis von GNU/LINUX-Installationen in der niedersächsischen Finanzverwaltung gelungen. Auch die niedersächsische Polizei hatte in den letzten 12 Jahren mit etwa 12.000 Arbeitsplätzen (bei über 22.000 Mitarbeitern) erfolgreich diesen Wechsel vollzogen. Diese Strategie hat das niedersächsische Innenministerium zu meinem großen Bedauern Ende 2014 beendet. Begründet wurde dies mit dem Umstand, dass neben der strategischen LINUX-Plattform für Clients im Lauf der Jahre die Beschaffung und der Parallelbetrieb mehrerer tausend Windows-Rechner erfolgt sei und nunmehr aus Gründen anzustrebender Personalsynergien im Bereich des Entwicklungs- und Administrationsbetriebs eine Ein-Plattformstrategie zu Gunsten der Microsoft-Linie verfolgt werden solle. Mir liegen keine Informationen vor, inwieweit die oben genannten Aspekte zur Informationssicherheit und zur Einhaltung datenschutzrechtlicher Vorschriften und technisch-organisatorischer Anforderungen in die Bewertung eingeflossen sind. Antworten der Projektleitung auf erste Nachfragen meiner Behörde konnten hier noch nicht abschließend bewertet werden, weil mir bis zum Ende des Berichtszeitraumes weder Schutzbedarfsfeststellung, noch Risikoanalyse, noch Wirtschaftlichkeitsuntersuchung oder Vorabkontrolle mit substantiellen Aussagen zur Informationssicherheit und zur datenschutzrechtlichen Bewertung dieser groß dimensionierten Migrationsplanung im Rahmen einer Unterrichtung nach § 22 Abs. 2 NDSG vorgelegt worden sind.

6. Ende-zu-Ende-Verschlüsselung konsequent nutzen

Mit der Erkenntnis, dass bei der Datenübermittlung innerhalb oder zwischen IT-Verfahren bzw. innerhalb oder zwischen öffentlichen Stellen (Behörden, Dienststellen, Körperschaften, Anstalten und Stiftungen) stets verschiedene Angriffsvektoren drohen, stellt sich die Frage, wie dieser Bedrohung begegnet werden kann. Die wirksamste Konzeption für Vertraulichkeit und Integrität ist bekanntermaßen die Verschlüsselung. Diese muss jedoch unter der Kontrolle der Kommunikationspartner am jeweiligen Ende der Kommunikationsstrecke liegen, ohne dass ein Intermediär auf einem Zwischenabschnitt die Kontrolle vorzeitig übernehmen kann (Ende-zu-Ende-Verschlüsselung). Diese nicht neue Forderung hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zuletzt im März 2014 in Hamburg mit der Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation" formuliert und näher ausgeführt.[4]

4 Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März in Hamburg: „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation", http://www.lfd.niedersachsen.de/download/85979; inhaltlich wird darin u. a. die Prüfung und Umsetzung folgender Maßnahmen gefordert: 1. Sichere Verschlüsselung beim Transport und bei der Speicherung von Daten, 2. Bereitstellung einer einfach bedienbaren Verschlüsselungs-Infrastruktur, 3. Einsatz von Ende-zu-Ende-Verschlüsselung in Kombination mit Verfahren zur Verbindungsverschlüsselung, 4. Sichere und vertrauenswürdige Bereitstellung von Internetangeboten, 5. Weiterentwicklung innovativer Vorkehrungen zum Schutz von Verkehrsdaten, 6. Ausbau der Angebote und Förderung anonymer Kommunikation, 7. Angebot für eine Kommunikation über kontrollierte Routen, 8. Sichere Verschlüsselung der Mobilkommunikation und Einschränkung der Möglichkeiten der Geolokalisierung, 9. Beschränkung des Cloud Computing mit personenbezogenen Daten auf vertrauenswürdige Anbieter mit zertifizierter Informationssicherheit, 10. Förderung der Vertrauenswürdigkeit informationstechnischer Systeme durch Zertifizierung, 11. Sensibilisierung von Nutzerinnen und Nutzern moderner Technik, 12. Ausreichende Finanzierung von Maßnahmen der Informationssicherheit. Der Arbeitskreis Technische und organisatorische Datenschutzfragen der Datenschutzkonferenz hat dazu einen Anforderungskatalog formuliert, der die genannten Maßnahmen konkretisiert und als Anlage zu dieser Entschließung existiert: http://www.lfd.niedersachsen.de/download/85980

IT-Planungsräte müssen Weichen neu stellen

Die Erkenntnis, dass es in öffentlichen Stellen zu einer kritischen Betrachtung der realen Informationssicherheit, des Schutzniveaus der eingesetzten Plattformen, der IT-Infrastruktur und der Systeme kommen muss, war eine zwingende Konsequenz – spätestens aus der NSA-/GCHQ-Spionageaffäre ab Juni 2013. Bereits im Sommer 2013 forderte ich in meiner beratenden Funktion – vertreten durch den dafür zuständigen Referatsleiter meiner Behörde – die Vertreter der Staatskanzlei und der Ministerien auf, im Interesse der Informationssicherheit und des Datenschutzes die gesamte IT-Architektur der Landesverwaltung zu überprüfen und die oben genannten grundlegenden Maßnahmen zu veranlassen. Zudem sollte die Frage der Vertrauenswürdigkeit, bezogen auf Hersteller, Provider, Dienstleister und die Hard- und Software-Produkte, ernsthaft und kritisch geprüft werden.
Auch im IT-Planungsrat[5] habe ich mehrfach darauf hingewiesen, dass Abweichungen von den Mindestanforderungen nicht verantwortbar seien, weil sonst eine Beherrschbarkeit der Risiken und Gefahren für die Grundrechte Betroffener nicht gewährleistet ist, und dass das Zulassen von Betriebsmodellen mit schwächeren Sicherheitsvorkehrungen den gesetzlichen Vorgaben des § 7 Abs. 1 NDSG zuwiderlaufe. Die Vertreter der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK)[6] haben letztlich auch gegenüber dem IT-Planungsrat Bund/Länder die Positionen aus den Entschließungen, die ab Juni 2013 zu den NSA-Spionageaktivitäten gefasst worden sind[7], bekräftigt.

Mobilgeräte nur mit sicheren Plattformen nutzen

Um Mobilgeräte wie Tablets und Smartphones für dienstliche Zwecke bei der Ausübung öffentlicher Aufgaben in öffentlichen Stellen sicher und datenschutzkonform betreiben zu können, sind zunächst die richtigen Rahmenbedingungen zu schaffen:

1. Der Einsatz eines Mobile Device Managements (MDM) bietet die organisatorische und die technische Plattform, um überhaupt Sicherheitsbedingungen und -vorgaben („Policy") auszugestalten und diese Regeln technisch zu implementieren. Damit werden diejenigen Geräte

5 In meinem XX. Tätigkeitsbericht 2009–2010, Seite 72 bis 77, unter dem Titel „IT-Management des Landes: Der Landesdatenschutzbeauftragte berät" habe ich die beratende Mitwirkung meiner Behörde grundlegend beschrieben.

6 Die DSK ist durch einen Vertreter der BfDI und einen Vertreter des Vorsitzes des Arbeitskreises Technik der DSK im IT-Planungsrat Bund/Länder mit beratender Stimme vertreten. Der IT-Planungsrat ist ein Gremium, das der politischen Steuerung für IT-Strategien bei Bund, Ländern und Kommunen gleichermaßen dient. Er hat vier Aufgaben: Koordination der IT-Zusammenarbeit von Bund und Ländern, Beschlüsse von IT-Interoperabilitäts- und IT-Sicherheitsstandards, Steuerung von Projekten der Nationalen E-Government-Strategie (NEGS) und Planung und Entwicklung des Verbindungsnetzes der öffentlichen Verwaltung. Rechtsgrundlage ist der auf Art. 91c Grundgesetz basierende IT-Staatsvertrag vom 27. Mai 2010 (https://www.bgbl.de/banzxaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl110s0662.pdf), der am 1. April 2010 in Kraft trat und durch die Länder durch Landesgesetzgebung ratifiziert (Niedersächsisches Gesetz vom 17. März 2010, Nds. GVBl. S. 142) worden ist.

7 Entschließungen der DSB-Konferenzen zum Grundrechtsschutz und zur Informationssicherheit anlässlich der Spionageaffäre: 88. Konferenz am 8./9. Oktober 2014: Entschließung „Effektive Kontrolle Nachrichtendienste" und Entschließung „Datenschutzaufsicht Grundrechtsschutz"; 87. Konferenz am 27./28. März 2014: Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation"; Anlage zur Entschließung „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation"; 86. Konferenz am 1./2. Oktober 2013: Entschließung „Forderungen für die neue Legislaturperiode: Die Datenschutzgrundrechte stärken!"; Entschließung „Handlungsbedarf zum Datenschutz im Bereich der Öffentlichen Sicherheit in der 18. Legislaturperiode des Deutschen Bundestages", Entschließung „Sichere elektronische Kommunikation gewährleisten – Ende-zu-Ende-Verschlüsselung einsetzen und weiterentwickeln"; Entschließungen zwischen den Konferenzen: Entschließung „Keine umfassende und anlasslose Überwachung durch Nachrichtendienste! Zeit für Konsequenzen" (5. September 2013); Entschließung „Geheimdienste gefährden massiv den Datenverkehr zwischen Deutschland und außereuropäischen Staaten!" (24. Juli 2013); Entschließung „Das Grundrecht auf informationelle Selbstbestimmung darf weder von inländischen noch von ausländischen Stellen verletzt werden!" (26. Juni 2013)

vom Zugang zu internen Datenbeständen und Datenverarbeitungsprozessen mit personenbezogenen Daten ausgeschlossen, die nicht die Vorgaben erfüllen.

2. Es sind gehärtete Betriebssysteme einzusetzen, das heißt, alle Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe durch das Programm nicht zwingend notwendig sind, müssen entfernt werden. Damit wird sichergestellt, dass ausschließlich dedizierte Software auf der Plattform verbleibt, die für den Betrieb des Systems nach definierten Festlegungen tatsächlich notwendig ist, und deren unter Sicherheitsaspekten bestimmungsgemäßer Betrieb und Funktionsablauf garantiert werden kann. Oftmals gelingt einem Angreifer der Einbruch in ein Gerät und in das Betriebssystem durch den Missbrauch eines Programms, das auf diesem Gerät gar nicht installiert sein müsste[8]. Dies gilt es zu vermeiden.
3. Es ist nur geprüfte und vom Betrieb zugelassene Anwendungssoftware (Apps) zuzulassen.
4. Lokale Datenspeicherungen sind weitestgehend zu verwenden.
5. Der Betrieb von Malwareschutz und Firewall ist unabdingbar.
6. Es sind VPN-Tunnelverbindungen zum Server der Dienststelle und zum IT-Dienstleister IT.N einzusetzen, um Seitenangriffe auf der Kommunikationsstrecke maßgeblich zu erschweren.
7. Inhaltsdaten sind zu verschlüsseln, und es bedarf eines ganzheitlichen Schlüsselmanagements.
8. Im Verlustfall muss die Möglichkeit der administrativen Fernlöschung bestehen.

Landesprojekt MDM mit Mängeln im Ansatz

Ich konnte mich davon überzeugen, dass in der Landesverwaltung die Erkenntnis vorhanden ist, für mobile Endgeräte vor Inbetriebnahme besondere technische und organisatorische Schutzmaßnahmen durchzuführen. Das trifft einmal auf den Betrieb mit Internetzugang zu, aber vor allem auch auf die Einrichtung des Zugangs in das Landesnetz und auf die Server, Funktionen und Datenbestände der Landesverwaltung. Die Kombination beider Zugänge stellt eine Potenzierung der Gefährdungen dar.

Es wurde daher ein Projekt MDM (Mobile Device Management) beim Landesbetrieb IT.Niedersachsen eingerichtet[9]. Dabei sollten folgende Betriebssysteme unterstützt werden:

- iOS 7.x und höher,
- Android 4.x und höher,
- Windows Phone 8.x und höher,
- BlackBerry 5.x und 10.x und höher.

8 Leitfaden Informationssicherheit IT-Grundschutz kompakt, BSI, 29. März 2012, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile

9 Projekt MDM des IT.N, http://www.it.niedersachsen.de/startseite/dienstleistungen/themen_und_projekte/mobile-device-management---mit-sicherheit-mobil---125419.htm

Ende 2013 befanden sich etwa 500 mobile Endgeräte im Einsatz, darunter etwa 300 Blackberry-Geräte. Die 200 Apple-iOS-Geräte wurden mit der Lösung McAfee Enterprise Mobility Management Konsole (McAfee EMM) verwaltet. Für die neue MDM-Lösung ab Ende 2013 wurde als Produkt das Managementsystem der US-Firma MobileIron[10] ausgewählt, mit dem die Endgeräte und die Software auf Basis einer SQL-Datenbank verwaltet werden. Die neue Lösung integriert mobile Endgeräte mit unterschiedlichen Betriebssystemen. Laut Projektbeschreibung geht IT.N davon aus, dass sie diese zuverlässig absichert. Die im Rechenzentrum des IT.N betriebene zentrale Konsole ermöglicht das Management aller dort betreuten mobilen Endgeräte in Echtzeit. Inhalte von Dateiablagen und Apps können kontrolliert zur Verfügung gestellt und Zugriffsrechte auf E-Mail-Accounts geprüft vergeben werden. Sicherheitsrichtlinien werden automatisiert auf die mobilen Geräte aufgebracht. Falls Bedarf nach erhöhten Sicherheitsanforderungen besteht, können in enger Abstimmung mit dem Kunden kundenspezifische Sicherheitspolicies realisiert werden.
Im Rahmen der Beratung nach § 22 NDSG ließen sich im Januar 2014 Vertreter meiner Behörde die konzeptionellen Planungen des Projektes und die bisherigen technischen Einzelheiten zur Ausgestaltung der Endgeräte, der Policy und der zentralen Administrationsfunktionen erläutern. Dabei enstand der Eindruck, dass die Projekt- und Betriebsverantwortlichen zwischenzeitlich ein tendenziell hohes Sicherheitsbewusstsein entwickelt hatten. Allerdings werden geplante regulierende Ansätze recht häufig durch den hohen Erwartungsdruck der Anwender in Kenntnis der Funktionsvielfalt heutiger Geräte und durch den Wunsch nach dem „Neuesten" in Frage gestellt. Statt durch administrative Regulierung mittels Policies für Informationssicherheit und Datenschutz zu sorgen, wird allzu leicht dem Komfortwunsch nachgegeben, und es kommt zu Kompromisslösungen. Das widerspricht dem Gedanken einer Systemhärtung. Hier halte ich eine klare strategische Positionierung zu Gunsten der Informationssicherheit und des Datenschutzes und eine bessere flächendeckende Aufklärung der Beschäftigten über die Risiken für unabdingbar. Dies liegt in der Verantwortung der zentralen Projektierung (Innenministerium und IT.N), aber auch der Ressorts und Behörden auf der Kundenseite, die Bedarfsträger und verantwortliche Stellen für die Festlegung der Policies sind. Die Informationssicherheitsbeauftragten und die behördlichen Datenschutzbeauftragten sollten hier gezielte Aufklärungs- und Durchsetzungskampagnen konzipieren (so genannte Awareness-Kampagnen).
Bei den Fachgesprächen mit der Projektleitung sprachen meine Mitarbeiter insbesondere folgende Probleme an:

- Bring Your Own Device (BYOD) mit nicht lösbaren rechtlichen Problemen und praktischen Datenhaltungskollisionen (siehe Beitrag auf Seite 40 zu IT-Systemen in Schulen[11]).
- Problem der uneinheitlichen Einsatzszenarien, damit müsste die höchste anzunehmende Schutzbedarfsfeststellung den Schutzbedarf insgesamt bestimmen.
- Fehlende Härtung der Geräte (s.o.).
- Betrieb von Sicherheitsfunktionen auf unsicherer Betriebssystemplattform; es wurde dabei auch von Seiten meiner Behörde auf Alternativprodukte wie z. B. SiMKo3 oder SecuSUITE hingewiesen, die bereits ein Konzept mit vollständigen Sicherheitsfunktionen mitbringen und vom BSI empfohlen werden[12]. Zudem wird seitens des BSI ein alternativer Ansatz namens „Systemlösung" als Strategie favorisiert: Weil der Smartphone-Markt sehr schnelllebig sei und die Evaluierung und Entwicklung sicherer Endgeräte viel Zeit in Anspruch nehme, werde es immer schwieriger, sichere Endgeräte bereitzustellen, bevor die Geräte wieder als veraltet be-

10 MobileIron Corp., Mountain View, Kalifornien, USA, http://www.mobileiron.com/
11 Vgl. Beitrag Seite 128 „Mobile Endgeräte: Trackende Datenschnüffler und allwissende Verräter", Aussage zu privaten Endgeräten im Abschnitt „Lehrkräfte auch durch praktische Trainings qualifizieren"
12 „Sicheres mobiles Arbeiten", BSI, Erscheinungsdatum 1. Februar 2014, Seiten 16 bis 29; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Sicheres-Mobiles-Arbeiten_pdf.html

trachtet werden. Daher werde die Lösung in der Managementzentrierung gesehen, die die Security-Policies bestimme.
- Container-Lösung für Daten.
- Eine Reihe von Sicherheitsrisiken mit der Folge möglicher Datenschutzrechtsverletzungen.

Ich werde das Projekt wegen der potentiell flächendeckenden Ausbreitung und der ubiquitären Einsatzszenarien weiterhin rechtlich und technisch begleiten und mir angesichts der sich schnell verändernden technischen Innovationen eine Prüfung vorbehalten.

Noch offene Fragen zum Projekt NiC

Im Rahmen der Beratung begleitet meine Behörde weiterhin das Projekt Niedersachsenclient (NiC) als Nachfolgeprojekt des Projektes Desktopmanagement[13]. In zahlreichen Gesprächen konnten viele datenschutzrechtliche Auswirkungen, die vorwiegend durch neue Funktionen und architekturbedingte Änderungen der Version Windows 8.1 auf den neuen Clients verursacht wurden, intensiv diskutiert und bewertet werden. In fast allen Fragen konnten schließlich einvernehmliche Lösungen gefunden werden. Dazu gehörten Konfigurationsfragen zu vorbereiteten Cloud-Funktionen, bei denen das Problem der Vermeidung von Datentransfers in unsichere Drittländer zu lösen war. Es bleiben aktuell offene Fragen beim Vertragswesen (s. o.), der Online-Hilfe, die gegenüber der früheren Offlinehilfe als Standard eingestellt ist, sowie bei einigen grundlegenden Online-Anbindungen von Windows 8.1, die sich tendenziell bei der Nachfolgeversion 10 noch verschärfen dürften. Auch der Virtualisierungsansatz für das Desktop-basierte Internet-Browsing (s. o.) wurde leider nicht realisiert. Zu diesem Projekt wird auf den gesonderten Beitrag in diesem Bericht verwiesen.[14]

Wirtschaftlichkeitsgedanke nachrangig gegenüber Informationssicherheit und Datenschutz

Die Landesregierung betonte in allgemeinen Zielformulierungen bei der IT-Strategie klar und unmissverständlich, dass dem Datenschutz bei der Gestaltung der IT-Infrastruktur des Landes Niedersachsen eine große Bedeutung zukomme. Auf eben diese hervorgehobene Bedeutung des Datenschutzes möchte ich besonders eingehen. Sie manifestiert sich im Grundrecht der informationellen Selbstbestimmung[15], im Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme als Bestandteil des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG[16]) und in der angemessenen Ausgestaltung der technisch-organisatorischen

13 LfD Niedersachsen, XXI. Tätigkeitsbericht 2011–2012, Seite 93ff, Beitrag „Outsourcing des Desktopmanagements: Land nimmt schleichenden Kontrollverlust in Kauf"
14 siehe Beitrag Seite 174: „Windows 8.1 in der Landesverwaltung: Kein Konzept gegen neue Bedrohungen"
15 Grundrecht auf Informationelle Selbstbestimmung, Urteil des Ersten Senats vom 15. Dezember 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1
16 Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, Urteil des BVerfG vom 27. Februar 2008, Az. 1 BvR 370/07 und 1 BvR 595/07

Schutzmaßnahmen für Prozesse, IT-Systeme und personenbezogene Daten gemäß den einfachgesetzlichen Bestimmungen[17]. Dieser Hinweis erscheint mir deshalb angebracht, weil in der praktischen Umsetzung von Projektplanungen, bei Systementscheidungen und bei Beschaffungen häufig Grenzen betont werden, die sich aus dem Haushalt und aus der grundgesetzlich festgelegten Schuldenbremse ergäben. Zudem wird als besonders relevant in den Vordergrund gestellt, dass Wirtschaftlichkeitsüberlegungen Begrenzungen für Aufwände aufzeigen müssten.
Es liegt auf der Hand, dass der Sicherstellung des Grundrechtsschutzes von Bürgern und Beschäftigten das Primat zukommt. Zwar könnten IT-Verfahren unter dem Gesichtspunkt der Informationssicherheit bei risikobasierter Bewertung mit einem „vertretbaren Restrisiko" unter Umständen in den Echtbetrieb genommen werden, bei datenschutzrechtlich bewerteter Analyse eines hohen oder sehr hohen Schutzbedarfes und bei hohem oder häufig anzunehmenden Schadenseintritt durch Grundrechtsverletzungen ist ein solches Restrisiko dagegen nicht zulässig. Wirtschaftlichkeitsüberlegungen mit der Begründung „zu hoher Kosten für die erforderlichen Datenschutzmaßnahmen" können folglich zwar zu einem Verzicht auf ein IT-Verfahren oder bestimmte Technologien führen, sie können aber nicht ein Hinwegsetzen über die Anforderungen rechtfertigen. Ich empfehle daher, im Interesse einer grundrechtskonformen Auslegung diese Grundsätze explizit zur Handlungsmaxime zu machen und im Grundsatz einem Wirtschaftlichkeitsgedanken unterzuordnen.

Kriterienkatalog für Hersteller, Dienstleister und Produkte entwickeln

Bereits im XIX. Tätigkeitsbericht[18] wurde die Bedeutung von Datenschutz und Informationssicherheit hervorgehoben und festgestellt, dass aus Sicht meiner Behörde weiterhin das Angebot der grundlegenden Zusammenarbeit mit dem CISO und dem LSKN (heute IT.N) besteht, um den technischen Datenschutz mit einem systematischen Informationssicherheitsmanagement zu koordinieren. Die bisherigen Schutzmaßnahmen der Landesregierung (insbesondere gemäß Cyber-Sicherheitsstrategie mittels mehrstufig redundanter Firewall-Systeme, Spam-Filter, Application Security Gateways etc.), die Einführung eines vollumfänglichen Informationssicherheitsmanagementsystems (ISMS) nach Beschluss des Landeskabinetts im Jahr 2012 und die praktizierte fortlaufende Anpassung der Technologien sind grundsätzlich auch aus Sicht des Datenschutzes zu begrüßen. Meines Erachtens ist jedoch angesichts der Bedrohungslagen im IT-Umfeld erheblich beim personellen Aufwand für die Informationssicherheit nachzubessern.
Mit der Abkehr von der Vergabe großer zentraler Funktionsbereiche wie Desktopmanagement und TK-Betrieb an gewerbliche Dritte entsprach die Landesregierung erfreulicherweise im Ergebnis meinen Kritikpunkten und Forderungen nach Rückgewinnung der Kontrolle der verantwortlichen Stellen über Informationstechnik, Prozesse und Daten[19]. Insbesondere bei strategischen Planungen für die Zukunft sollten die Optimierungspotentiale und erweiterten Strategieaspekte nach meiner Ansicht noch ergänzt werden:
Ein effektiver Datenschutz bei der Entwicklung (Privacy by Design) und dem Betrieb von IT-Verfahren kann nur erreicht werden, wenn er auf einer validen Informationssicherheit (einschließlich der IT-Sicherheit) aufbauen kann, die wiederum nur prozesshaft erreicht werden kann. Anforderun-

17 Z. B. § 7 Abs. 1 NDSG, § 9 BDSG, § 78 a SGB X, § 13 Abs. 4 TMG, § 109 Abs. 2 TKG
18 XIX. Tätigkeitsbericht 2007–2008, Seiten 60 f., Kapitel 3. Schwerpunkt, 2. Informationssicherheit und technischer Datenschutz, http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=12917&article_id=56136&_psmand=48
19 Siehe z. B. XX. Tätigkeitsbericht 2009–2010, S. 102 f., „Des Kaisers neue Provider", und XXI. Tätigkeitsbericht 2011–2012, S. 93 ff., „Outsourcing des Desktopmanagements", http://www.lfd.niedersachsen.de/ > Navigation > Allgemein > Tätigkeitsberichte

gen der Informationssicherheit müssen dabei immer gegen die datenschutzrechtlichen Regelungen abgewogen werden und ergänzen sich im Idealfall. Hier entstehen bei rechtskonformer Handhabung rekursive Entwicklungs- und Changeprozesse. Den datenschutzrechtlichen Bedingungen und Auflagen ist dabei das ihnen grundrechtlich garantierte Primat zuerkannt, wie auch die Rechtsprechung des Bundesverfassungsgerichts deutlich macht, das in der praktischen Umsetzung von Strategien und operativem Betrieb beachtet werden muss.
Im Ergebnis empfehle ich dringend die Erarbeitung von Vertraulichkeitskriterien und die intensive Befassung mit Herstellern und Dienstleistern von Hard- und Softwareprodukten, gemessen an den eingangs dargestellten Kriterien, insbesondere der Standardtechnologien und -plattformen. Eine auf diese Weise entwickelte und verifizierte IT-Sicherheitsarchitektur halte ich für unabdingbar, um standardisierbare Risikofaktoren sachgerecht berücksichtigen zu können.

Privacy by Design und Privacy by Default strategisch verbindlich festlegen

In allen Architekturfragen der IT-Planung und auch in der Entwicklung und im Betrieb von IT-Verfahren sollte der Privacy-by-Design-Ansatz in die Implementierung Einzug halten. Dieser Grundsatz hilft zu verhindern, dass Schutzmaßnahmen mit überhöhtem Aufwand in späteren Betriebsphasen nachgebessert werden müssen. Stattdessen wird bereits in der Designphase – zum Beispiel bei der Wahl und Härtung von Betriebssystemplattformen, der Gestaltung beim Datenbankdesign zur Mandantenfähigkeit oder bei der Entwicklung eines ganzheitlichen und systematisierten Rechte-/Rollen-Konzepts – die Grundlage für ein ausbaufähiges Datenschutz- und Informationssicherheitskonzept geschaffen. In dieser Privacy-by-Design-Phase sollten neben der datenschutzrechtlichen Anforderung der Datensparsamkeit die sechs elementaren Gewährleistungsziele[20] subsumiert werden. Das heißt, durch Beachtung der Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit sowie dem datenschutzrechtlichen Grundsatz der Datensparsamkeit werden alle Grundlagen für datenschutzkonforme Ausgestaltungen der IT-Verfahren erreicht. Würde dies bereits in der Designphase angewandt und beachtet, entfielen viele Mängel oder sogar eine Design-bedingte Verhinderung von Datenschutzmaßnahmen, zumindest bei Produkten und IT-Verfahren.
Auch die Ausgestaltungen technischer (Privacy-by-Default-Ansatz bei der Auslieferung an den Betrieb und bei der Administration) und organisatorischer Natur auf Seiten der verantwortlichen Stelle und der beauftragten Entwickler (Customizing, Solution-Anbieter etc.) bleibt eine zusätzliche Aufgabe, die jedoch bei Beachtung des Privacy-by-Design-Ansatzes erheblich geringer oder zumindest schlüssiger umsetzbar wäre. Zusammenfassend

20 Vgl. Beitrag Seite 184 „Elementare Gewährleistungsziele: Das Standard-Datenschutzmodell nimmt Konturen an"

empfehle ich dringend, die Grundsätze Privacy by Design und Privacy by Default in den jeweiligen Entwicklungs- und Betriebsphasen strategisch verbindlich festzulegen.

Mehr Personal für N-CERT nötig

Die Instanz eines N-CERT (Niedersachsen Computer Emergency Response Team) als zentrale Stelle für Abwehr und Koordinierung von IT-Sicherheitsvorfällen halte ich für eine wichtige zentrale Einrichtung zur Förderung eines bewerteten Lagebildes zur Informationssicherheit, von dem auch das Schutzniveau für technisch-organisatorischen Datenschutz profitiert. Neben dem Erstellen eines Sicherheitslagebildes ist es Aufgabe des N-CERT,

- den Landesbehörden Unterstützung bei der Sicherheitsvorfallbehandlung zu gewähren,
- die Koordination ressortübergreifender Sicherheitsvorfälle zu übernehmen,
- Aufgaben der Sicherheitsberatung und von Risikoanalysen wahrzunehmen sowie
- einen Warn- und Informationsdienst sicherzustellen.

Allerdings halte ich die personelle Ausstattung mit bisher drei Personen angesichts der zu bewältigenden Aufgaben für unangemessen niedrig. Zudem ist eine Verdichtung von Informationsflüssen und eine Optimierung der strategischen und operativen Informationsvernetzung mit den behördlichen Datenschutzbeauftragten von Land und Kommunen sowie mit meiner Behörde dringend geboten. Das zwischen Land und Kommunen geplante ebenenübergreifende Cyber-Sicherheitsbündnis ist insofern ein überfälliger Schritt zur Stärkung nicht nur des Informationssicherheitsmanagements, sondern auch der Erkenntnislage und der operationalen Reaktionsfähigkeit auf Sicherheitsvorfälle. Jede frühzeitige sachgerechte Abwehrmaßnahme und jede koordinierte Nachsteuerung der Informationssicherheit kommt auch dem Datenschutz zu Gute.

TK-Infrastruktur, e-Akte, Anonymisierung, Verschlüsselung: Beratende Funktion im Niedersächsischen IT-Planungsrat

Wie in den Vorjahren hat meine Behörde bei den Entscheidungen des Niedersächsischen IT-Planungsrates[1] auch 2013 und 2014 wieder regelmäßig beratend mitgewirkt. Dies geschah und geschieht zu einem erheblichen Teil mit Blick auf die technisch-organisatorischen Aspekte, aber auch auf die materiellrechtlichen Beurteilungen der Standardisierung von IT und der Implementierung von IT-Verfahren und -Infrastrukturen in der Landesverwaltung.

Einen breiten Raum meiner datenschutzrechtlichen Beratung und Kontrolle im Zusammenhang mit den IT-Strategien der Landesverwaltung und des Niedersächsischen IT-Planungsrates nehmen Themen in Anspruch, die durch die Informationssicherheit geprägt sind, die zunehmend an Bedeutung gewinnt (siehe hierzu auch den Beitrag „Informationssicherheit in Behörden und Kommunen gefährdet", Seite 152). Nachfolgend beschreibe ich exemplarisch einige IT-Planungsrat-Themen, mit denen sich mein Haus aus datenschutzrechtlicher Sicht befasst hat:

Zahlreiche Anregungen zur neuen Telekommunikations-Infrastruktur

Für die Landesverwaltung plant das niedersächsische Innenministerium (MI) seit einigen Jahren eine Modernisierung des Telekommunikationsnetzes (z. B. LAN, MAN, WAN, TK-Anlagen) einschließlich der aktiven und passiven Übertragungsstrecken sowie der Telekommunikationsdienste wie zum Beispiel Verzeichnisdienste, Sprachkommunikation, Videokonferenzdienste und Kollaboration. Dabei wurde als Ziel ein einheitliches IP-basiertes Netz für die Integration aller Kommunikationsformen (Telefonie per Voice over IP – VoIP, Datentransfer, Internetzugang, E-Mail-Verkehr usw.) definiert, um mit einer einheitlichen technischen Basis und einer weitgehend homogenen Administration zu einem kostengünstigen Betrieb zu gelangen.
Zu Beginn des Umsetzungsprojektes Niedersachsen Next-Generation-Network (NI-NGN) im März 2009 war noch vorgesehen, mit Hilfe eines Konsortiums unter Führung der Firma EWE Tel 75.000 Anschlüsse in 2.500 Dienststellen in einem einheitlichen, effizienten und sicheren Netzwerk zu realisieren. Ende 2012 hatte das MI nach verschiedenen Umsetzungsschwierigkeiten offiziell eine im gegenseitigen Einvernehmen vorgenommene umfangreiche Reduzierung des Rahmenvertrages TK2010 zum Aufbau und Betrieb bekanntgegeben. Zur Einschätzungen meiner Behörde zu den datenschutzrechtlichen Risiken einer derart weitgehenden Auftrags-

1 Vgl. umfassender Beitrag zum Niedersächsischen IT-Planungsrat im XX. Tätigkeitsbericht 2009–2010, Kapitel 3, Technisch-organisatorischer Datenschutz, „IT-Management des Landes: Der Landesdatenschutzbeauftragte berät", Seiten 72 f.

vergabe verweise ich auf den XXI. Tätigkeitsbericht (Seite 93). Die Fortführung des Modernisierungsprojektes wurde 2013 dem IT.Niedersachsen (IT.N) übertragen. Im Rahmen der Sitzungen der Arbeitsgruppe TK-Strategie zur TK-Infrastruktur hatten meine Mitarbeiter in den Stellungnahmen auf datenschutzrechtliche Anforderungen und Schutzmaßnahmen in einem integrierten neuen TK-Betrieb hingewiesen, insbesondere auf Verschlüsselung zum Schutz IP-basierter Sprachübertragung (VoIP-Telefonie). Dies erfolgte in der Fortsetzung der langjährigen Begleitung zu den Planungen des ehemaligen Projektes „izn-Net“[2]. Zahlreiche Anregungen fanden Eingang in die konzeptionellen Planungen.

Der zur Sitzung des Niedersächsischen IT-Planungsrats am 30. Juli 2014 vorgelegte „Umsetzungsplan zur TK-Strategie für die Landesverwaltung Niedersachsen“ wurde bis zur Sitzung am 13. November 2014 von den Ressorts und unter Beteiligung meiner Behörde einvernehmlich überarbeitet. Dies betraf insbesondere Ergänzungen aufgrund ressortspezifischer Belange sowie die in der Stellungnahme meines Hauses vom 19. September 2014 dargelegten Empfehlungen. Der Niedersächsische IT-Planungsrat fasste daraufhin folgenden Beschluss:

1. Der Niedersächsische IT-Planungsrat nimmt den vom Landesbetrieb IT.Niedersachsen vorgelegten „Umsetzungsplan zur TK-Strategie für die Landesverwaltung Niedersachsen“ zur Kenntnis.
2. Der Niedersächsische IT-Planungsrat stimmt der geplanten Vorgehensweise zu, dass die ressortspezifische Umsetzung der TK-Strategie im Einvernehmen mit den betreffenden Ressorts nach Klärung der organisatorischen, technischen und haushaltswirtschaftlichen Rahmenbedingungen mit dem Ziel einer weitgehenden Standardisierung und Automatisierung erfolgt.
3. Der Niedersächsische IT-Planungsrat beauftragt MI, auf der Basis des „Umsetzungsplans zur TK-Strategie für die Landesverwaltung Niedersachsen“ den Landesstandard für die Netzinfrastruktur in Abstimmung mit den Ressorts zu entwickeln.
4. Der Niedersächsische IT-Planungsrat bittet MI, die haushaltsmäßigen Auswirkungen des „Umsetzungsplans zur TK-Strategie für die Landesverwaltung Niedersachsen“ zur 22. Sitzung am 16. April 2015 darzustellen.

Bei der Fortsetzung der TK-Planungen und Implementierungen werde ich mit meiner Behörde weiterhin datenschutzrechtlich und IT-fachlich die Umsetzungsmaßnahmen begleiten und prüfen.

Anonymisierung der arbeitsplatzbezogenen IP-Adressen dringend geboten

Da in IP-Netzen einzelnen Geräten, die an das Netz angebunden sind, eine eigene IP-Adresse zugewiesen wird, sind die Geräte individuell identifizier-

2 Vgl. XVIII. Tätigkeitsbericht 2005-2006, Seite 55, im Kapitel „Beteiligung bei IT-Verfahren des Landes und der Kommunen/2. „mit.niedersachsen“ – mit Datenschutz“

bar, adressierbar und damit erreichbar. Die IP-Adresse kann folglich einen einzelnen Empfänger oder eine Gruppe von Empfängern identifizieren. Es ist daher davon auszugehen, dass IP-Adressen personenbeziehbar sein können. Eine Offenlegung ist als datenschutzrechtliches Risiko zu bewerten. Erstrebenswert ist eine Anonymisierung der landesinternen IP-Adressen beim Datenaustausch über das Internet.
Zunächst ist zu begrüßen, dass die IT-Arbeitsplätze mit dem Internet über eine Landesfirewall abgesichert sind und diese über eine sogenannte Proxyfunktionalität (zentraler Proxyserver) verfügt, die landesinterne Webanfragen entgegennimmt, um dann über ihre eigene Adresse eine Verbindung zur Gegenstelle im Internet herzustellen.
Der zentrale Proxyserver des Landes Niedersachsen kann aber zusätzlich mithilfe eines sogenannten X-Forwarded-For-Headers (XFF-Header) die landesinterne IP-Adresse des Arbeitsplatz-PCs an die Gegenstelle im Internet übermitteln. Diese Option wird genutzt, ist aber nur einheitlich für alle Arbeitsplatz-PCs aktivierbar oder deaktivierbar. Aufgrund der genannten Risiken wäre die Abschaltung des XFF-Headers, die den zentralen Proxyserver des Landes zu einem Anonymisierungsdienst macht, dringend geboten, um nur die zentrale und nicht personenbeziehbare IP-Adresse des Landes an das Internet zu übertragen.
Um bestimmte Fachverfahren, die die landesinterne IP-Adresse zur Authentifizierung nutzen, in ihrer Funktionalität nicht zu beeinträchtigen, müssen für diese Fachverfahren vor Abschaltung des XFF-Headers Alternativlösungen gefunden werden. Dies sollte in den nächsten Monaten des Jahres 2015 erfolgen, und es sollten mit Nachdruck alternative Authentifizierungsverfahren geprüft werden. Ich forderte in diesem Zusammenhang auch eine baldige Beendigung der IP-basierten Identifizierung und wies darauf hin, dass zum Teil auch Webshops diese vergleichbar günstige Form der Identifizierung nutzen. Der IT-Planungsrat fasste daher im November 2014 den Beschluss, das Ziel der Anonymisierung der landesinternen IP-Adressen durch die zentrale Landesfirewall zu verfolgen. Die Ressorts wurden gebeten, die Fachverfahren, die eine personenbezogene IP-Adresse zur Authentifizierung nutzen, auf alternative Authentifizierungsverfahren zu überprüfen. Das MI soll bis April 2015 einen Umsetzungsplan vorlegen.

Elektronische Aktenführung: Geändertes Konzept birgt Gefahren

Ziel des Projektes eAkte Niedersachsen ist es, eine flexible und leicht handhabbare, kollaborative Benutzeroberfläche zu schaffen und diese in einem ersten Schritt mit den Funktionalitäten eines Ablage- und Registrierungssystems zu verbinden. Die Landesregierung hatte Ende 2012 beschlossen, das Projekt zur Einführung der elektronischen Aktenführung in der Landesverwaltung unter Nutzung des Dokumentenmanagementsystems (DMS) „eGov-Suite“ der Fa. Fabasoft zum Ende der Pilotphase zu beenden.
Die Fortsetzung der elektronischen Aktenführung soll nunmehr mit einem geänderten Konzept erfolgen. Für die Fortschreibung wurde ein auf dem Produkt SharePoint der Fa. Microsoft basierendes DMS empfohlen. Das MI soll nach Ablauf der Pilotphase einen Erfahrungsbericht inklusive einer Wirtschaftlichkeitsbetrachtung zur schrittweisen Einführung einer elektronischen Aktenführung in der niedersäch-

sischen Landesverwaltung vorlegen. In weiteren Schritten sollen insbesondere eine vollständige Office-Integration sowie ein möglichst unkompliziertes Vorgangsbearbeitungssystem (VBS) in Form einer „elektronischen Umlaufmappe" bereitgestellt werden. Die Software-Architektur der auf der Basis von SharePoint 2013 entwickelten Standardanwendung NI-DMS ist entsprechend dem Konzept E-Verwaltung so konzipiert, dass sie dem Anwender oder der Anwenderin drei Ablagemöglichkeiten (Handaktenbereich, Arbeitsablage, verlässliche Aktenablage) bietet.
Mit der Wahl des Produktes MS SharePoint ist meines Erachtens eine weitere Festlegung getroffen worden, die das Risiko der Produktabhängigkeit mit sich bringt (siehe hierzu meinen separaten Beitrag „Informationssicherheit in Behörden und Kommunen gefährdet", Seite 153). Dies könnte sich in der engen Verflechtbarkeit dieses E-Akte-Verfahrens mit zahlreichen Microsoft-Produkten wie MS-Windows (Betriebssystem), MS-Office (Bürofunktionalitäten), MS-Exchange/Outlook (E-Mail) manifestieren.
Da ich in die aktuelle Planungsphase zur Einführung von MS SharePoint nicht eingebunden war, bat ich im November 2014 um Beteiligung angesichts dieser und anderer mit dem Einsatz von SharePoint verbundenen Risiken. Dies wurde seitens der verantwortlichen Stelle (MI) zugesagt.

Verschlüsselte E-Mail-Kommunikation kommt

Für begrüßenswert halte ich einen Beschluss des Niedersächsischen IT-Planungsrates zur Einführung einer durchgängigen TLS-Verschlüsselung (Transport Layer Security) zwischen den E-Mail-Servern des Landes zum 1. Februar 2015. Die Ressorts wurden damit gebeten, in ihrem jeweiligen Zuständigkeitsbereich die verschlüsselte Kommunikation umzusetzen. Zudem wurde die Einführung einer durchgängigen so genannten RPC-Verschlüsselung zwischen den Arbeitsplatzrechnern und den E-Mail-Servern des Landes zum 1. August 2015 beschlossen. Die Ressorts müssen jetzt die Umsetzung in ihrem jeweiligen Zuständigkeitsbereich veranlassen.

Ende-zu-Ende-Verschlüsselung fehlt noch

Nach wie vor halte ich jedoch – zusätzlich zu den Verschlüsselungsinitiativen auf den Kommunikationsstrecken – eine vom Nutzer kontrollierte Ende-zu-Ende-Verschlüsselung auf der Inhaltsdatenebene für unabdingbar, weil dadurch eine nicht manipulierte und konsequente Integrität und Vertraulichkeit maßgeblich erreicht werden kann (siehe hierzu auch die Beiträge „Globale Überwachung durch Geheimdienste: Datenschutzbeauftragte in großer Sorge", Seite 12, und „Noch ein Vertrauensverlust: Der Heartbleed-Bug – Sicherheitslücke in einem Sicherheitsprotokoll", Seite 146).

Informationssicherheitsrichtlinie E-Mail: Innenministerium streicht Versandverbot für besonders schützenswerte Daten

Im Rahmen des Aufbaus eines ressortübergreifenden Informationssicherheitsmanagementsystems (ISMS) in der niedersächsischen Landesverwaltung hat das Niedersächsische Ministerium für Inneres und Sport am 1. August 2014 auf Basis der „Leitlinie zur Gewährleistung der Informationssicherheit in der Niedersächsischen Landesverwaltung (ISLL)“ die „Informationssicherheitsrichtlinie über die Nutzung des E-Mail-Dienstes (ISRL E-Mail-Nutzung)“ in Kraft gesetzt mit dem Ziel, die Inhalte bis zum 30. Juni 2015 zu realisieren. Zusätzlich wurde eine Musterdienstanweisung veröffentlicht.

In der Entwurfsfassung der ISRL war ein ausdrückliches Verbot des Versandes von Daten der Schutzstufen D und E vorgesehen. Aufgrund einer abweichenden Praxis in Teilen der Landesverwaltung (siehe Seite 182, „E-Mailverkehr in der Justizverwaltung“) wurde dieses Verbot ersatzlos gestrichen und durch einen knappen Verweis auf den Einsatz einer angemessenen Verschlüsselung ersetzt. Dies halte ich aus nachfolgenden Erwägungen für einen strategischen Fehler.

Mögliche Angriffe von außen und von innen

Grundsätzlich kommt eine Verarbeitung derart sensibler Daten nur auf Einzelplatzrechnern in Betracht. Bestenfalls kommt als Umgebung ein gesondertes lokales Netzwerk in Betracht, wenn umfangreiche Maßnahmen zur Absicherung insbesondere auch des Netzwerkes getroffen werden. Nach meiner Beurteilung des Schutzbedarfes, der Gefahren sowie der Eintrittswahrscheinlichkeit und der Schadenshöhe verbietet sich eine Verarbeitung derartiger Daten auf Rechnern, die über eine Internetanbindung verfügen, weil nicht ausgeschlossen werden kann, dass diese von Schadprogrammen befallen werden, die zudem eigenständig ins Internet kommunizieren könnten. Bei derart sensiblen Daten ist zudem auch der Angriff von innen, also aus dem lokalen Netz der Behörde, oder aus dem Landesnetz ein Risiko, das zuverlässig beherrscht werden muss. Hierbei ist gerade auch die Möglichkeit eines Angriffes über Fernwartungszugänge und Zugriffsmöglichkeiten für das Wartungspersonal zu berücksichtigen, denn dieses Szenario stellt ein zusätzliches Risiko dar. Darüber hinaus ist zu beachten, dass selbst im Falle einer rein hypothetischen Fehlerfreiheit und Sicherheit der eingesetzten Programme und Geräte der Anwender völlig frei in der Auswahl eines möglichen Mailempfängers ist und objektiv nicht jede Nachricht zwingend verschlüsselt wird.

Aus diesem Grunde muss mit Irrtümern und Tippfehlern gerechnet werden, die bereits in der Vergangenheit in der öffentlichen Verwaltung dazu geführt haben, dass Nachrichteninhalte ungewollt an Dritte weitergegeben wurden.

Musterdienstanweisung überfordert Anwender

Die Musterdienstanweisung verlangt vom Endanwender, Wesentliches zur IT-Sicherheit und dem Datenschutz durch Prüfung der eingegangenen Nachrichten beizutragen. Dies umfasst unter anderem folgende Forderungen:

1. **Der Anwender soll Angaben zum Absender und Inhalt auf Plausibilität prüfen**.
   Dies ist eine organisatorische Forderung, die kaum geeignet ist, dem Ziel der Informationssicherheit zu dienen.
   Tatsache ist, dass Absenderangaben im für den Mailversand genutzten SMTP-Protokoll ohne Weiteres gefälscht werden können. Tatsache ist ferner, dass die Headerfelder der Nachrichten innerhalb des Mailprogrammes MS Outlook, das in der Landesverwaltung mehrheitlich eingesetzt wird, standardmäßig nicht angezeigt werden und darüber hinaus für den normalen Anwender nur schwer zu interpretieren sind.
2. **Den Beschäftigten wird untersagt, ohne Genehmigung „Dateianhänge, die einen erkennbar ausführbaren Programmcode enthalten", zu öffnen.**
   Auch sämtliche Dateiformate der Office-Anwendungen (Word, Excel etc.) können regelmäßig Programmcode enthalten, ebenso wie die ebenfalls weitverbreiteten Formate „.pdf" und „.html". Auch wenn ein Verbot, diese Formate zu öffnen, erhebliche Teile des Mailversandes ad absurdum führen würde, ist aus technischer Sicht eine solche Differenzierung kaum nachvollziehbar, da von allen genannten Dateitypen vergleichbare Risiken ausgehen können (vergleiche zum Beispiel http://www.heise.de/newsticker/meldung/Patchday-Microsoft-schliesst-kritische-Office-und-IIS-Schwachstellen-2606628.html).
3. **„Personenbezogene Daten der Schutzstufen C, D und E […] dürfen nur dann elektronisch versandt werden, wenn die Vertraulichkeit der Informationen durch eine dem jeweiligen Schutzbedarf angemessene Verschlüsselung sichergestellt ist. […] Die Beschäftigten stellen im Fall von verschlüsselt versandten E-Mail-Anhängen sicher, dass Passwörter oder Entschlüsselungsschlüssel nicht in der betroffenen E-Mail selbst übertragen werden."**
   An anderer Stelle wird als mögliches Verschlüsselungsprogramm 7-Zip genannt. Angesichts der Tatsache, dass Adressat der Dienstanweisung die Beschäftigten einer Dienststelle sind, ist die Forderung einer „angemessenen Verschlüsselung" ungeeignet, da die mit durchschnittlichen IT-Kenntnissen ausgestatteten Beschäftigten in aller Regel nicht in der Lage sind, Verschlüsselungsverfahren fachtechnisch zu bewerten und insbesondere nicht in der Lage sind, selbst ein Verschlüsselungsprogramm auszuwählen. Aufgrund der Risiken bei der notwendigerweise unverschlüsselten Übermittlung von Kennworten sind symmetrische Verschlüsselungsverfahren für den E-Mail-Verkehr sensibler Daten grundsätzlich

ungeeignet. Insofern wären die Angaben zu einer „angemessenen Verschlüsselung“ zu konkretisieren, und der Hinweis über den Austausch von Kennworten wäre hinfällig.

Schutzbedarf nicht angemessen berücksichtigt

Eine Verarbeitung von Daten der Schutzstufe E auf Rechnern im Landesnetz ist nicht zuletzt aufgrund der Anbindung ans Internet grundsätzlich datenschutzrechtlich unzulässig. Ein Versand von Daten der Schutzstufe D kommt bestenfalls dann innerhalb des Landesnetzes und nur im Einzelfall in Betracht, wenn ein zuverlässiges System der asymmetrischen Ende-zu-Ende-Verschlüsselung und eine zentrale Verwaltung öffentlicher Schlüssel etabliert werden. Das Niedersächsische Datenschutzgesetz (NDSG) spricht mit gutem Grund von technisch-organisatorischen Maßnahmen zum Schutze personenbezogener Daten. Vorrangig hat der Schutz durch technische Lösungen zu erfolgen. Nur wenn diese nicht oder nicht mit nicht vertretbarem Aufwand realisierbar sind, kann an deren Stelle eine organisatorische Regelung treten.
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. Im Übrigen sollte die Musterdienstanweisung dahingehend überarbeitet werden, dass der Regelungsinhalt für die Adressaten hinreichend eindeutig und verständlich formuliert wird. An dieser Stelle besteht zumindest bei besonders vertraulichen Daten Nachbesserungsbedarf: Das Mailprogramm sollte durch Virtualisierung oder eine Terminallösung (zum Beispiel ReCoBS, vergleiche https://de.wikipedia.org/wiki/ReCoBS) gekapselt und gegebenenfalls landesinterner Mailverkehr und Mailverkehr über das Internet getrennt werden. Bundesbehörden mit entsprechendem Schutzbedarf setzen entsprechende Lösungen bereits seit Jahren ein.

Weitere Informationen:

Antwort der Bundesregierung auf Kl. Anfrage Bündnis90/Die Grünen: https://gruen-digital.de/wp-content/uploads/2015/04/Antwort-BR-FOSS.pdf, S. 6

Windows 8.1 in der Landesverwaltung: Kein Konzept gegen neue Bedrohungen

Das Land Niedersachsen sah sich für die Landesverwaltung durch die angekündigte Einstellung der Pflege von Windows XP und Office XP durch den Hersteller Microsoft gezwungen, auf eine modernere Softwareplattform umzusteigen. Die Einschaltung eines externen Dienstleisters führte vorrangig aus wirtschaftlichen Gründen nicht zum Erfolg, so dass die Landesregierung beschloss, die Umstellung in Eigenregie und in einem knappen Zeitrahmen selbst zu realisieren. Zu diesem Zweck kaufte das Land von Microsoft für einen sechsstelligen Betrag erweiterte Pflegedienstleistungen ein. Im Rahmen dieses Vertrages musste sich das Land verpflichten, auf eine Nachfolgeversion von Windows zu migrieren, ansonsten hätte Microsoft eine Unterstützung über den 8. April 2014 hinaus verweigert. Eine Prüfung datenschutzfreundlicherer Alternativprodukte war damit nicht möglich.

Aufgrund der sowohl zeitlich wie personell knappen Ressourcen musste sich das Projekt im Wesentlichen auf eine 1:1-Migration von Windows XP/Office XP auf Windows 8.1/Office 2013 beschränken. Das bedeutete, dass bei der Auswahl von Betriebssystem und der Office-Komponenten aufgrund der dargestellten vertraglichen Verpflichtungen datenschutzrechtliche Aspekte nicht mehr im vollen Umfang berücksichtigt werden konnten. Weiter waren Anpassungen an der im Wesentlichen mehr als ein Jahrzehnt alten Sicherheitsarchitektur, die mit der Einführung von Windows XP implementiert wurde, in der vorgegebenen Zeit nur sehr begrenzt realisierbar.

Gefahren durch Internetdienste und Sicherheitslücken

Für Informationssicherheit und Datenschutz bedeutet dies, dass zwar in Teilbereichen auch eine Verbesserung des Sicherheitsniveaus aufgrund der von Microsoft vorgenommenen Weiterentwicklung der Produkte im Hinblick auf Schutz vor Schadprogrammen eingetreten ist. Eine konzeptionelle Antwort auf die sich in der letzten Dekade entwickelten Bedrohungen ist jedoch unterblieben. Die grundsätzliche Bedrohung durch die Nutzung von Internetdiensten (E-Mail, Web und die inzwischen erhebliche Anzahl der durch HTTP getunnelten Protokolle) bleibt ebenso bestehen. Auch weiterhin wird von der Landesregierung akzeptiert, dass ein mehr oder minder großer Zeitraum verstreicht, bis die installierten Virenscanner mit aktuellen Signaturen versehen sind und neue Schadprogramme erkannt werden. Teilweise entstehen zudem objektiv sehr lange Wartezeiten, bis Sicherheitslücken in Programmen geschlossen werden. Wie auch Fachmedienberichten[1] zu entneh-

1 golem.de am 14. April 2015, http://www.golem.de/news/redirect-to-smb-uralte-sicherheitsluecke-in-allen-windows-versionen-1504-113476.html und Heise-online http://www.heise.de/security/meldung/Weiterleitung-auf-SMB-Freigabe-petzt-Passwort-Hash-2604952.html

men ist, handelt es sich dabei im schlimmsten Falle um Lücken[2] in sämtlichen Windowsversionen, die seit über 18 Jahren nicht geschlossen wurden.
Auch wenn derartige Meldungen eher die Ausnahme sind, vergehen doch regelmäßig Wochen, oft sogar Monate, bis Sicherheitslücken geschlossen sind. In dieser Zeit kann von einer Sicherstellung des Schutzes der verarbeiteten personenbezogenen Daten im eigentlichen Sinne, wie es § 7 Niedersächsisches Datenschutzgesetz (NDSG) fordert, nicht gesprochen werden. Da Virenscanprogramme sich mit weitreichenden Rechten tief im Betriebssystem verankern, stellen Sicherheitslücken in diesen Programmen eine erhebliche Bedrohung für die Sicherheit des betroffenen Systems dar, wie die jüngere Forschung ausgiebig diskutiert[3]. Hier bedarf es zumindest einer Prüfung, ob der Einsatz von Virenscannern innerhalb der normalen Systemumgebung noch ein beherrschbares Risiko darstellt, oder ob es hier zusätzlicher Sicherungsmaßnahmen bedarf.

Sicherheitsdomänen und Virtualisierung

Aufgrund der dargestellten Schwächen, die grundsätzlich alle am Markt verfügbaren Produkte betreffen, bedarf es einer Anpassung der Sicherheitsarchitektur: Es müssen unterschiedliche Domänen gebildet werden, deren Sicherheitsniveau dem Schutzbedarf der darin verarbeiteten Daten angepasst ist. Das bedeutet, dass insbesondere die Bedrohung des Browsers und des E-Mail-Programms bei der internetbasierten Kommunikation akzeptiert werden muss, während jedoch der Gefahr dadurch begegnet wird, dass die besonders bedrohten Programme weitgehend vom Zugriff auf sensible Daten abgeschirmt werden.
Ein etabliertes Verfahren hierfür ist die Kapselung derartiger Programme durch Virtualisierung. Hierzu laufen die potentiell bedrohten Anwendungen auf einem eigenen Betriebssystem entweder in einer virtuellen Umgebung auf dem Arbeitsplatzrechner oder sogar auf einem dedizierten Server in einem abgeschotteten Netzsegment. Sollte es einem Angreifer gelingen, die Sicherheitsvorkehrungen der Anwendung oder gar des darunterliegenden Betriebssystems zu überwinden, findet er sich nun vor

2 Heise-online am 14. November 2014, http://www.heise.de/newsticker/meldung/Exploit-bringt-Nutzer-aller-Windows-Versionen-in-Gefahr-2457372.html
3 Heise-online am 14. November 2014, http://www.heise.de/newsticker/meldung/Exploit-bringt-Nutzer-aller-Windows-Versionen-in-Gefahr-2457372.html

der weiteren Hürde der Virtualisierungsumgebung und der des Servers und hat von dort keinen oder nur sehr eingeschränkten Zugriff auf vertrauliche Daten. Entsprechende Konzepte werden bereits seit Jahren vom Bundesamt für Sicherheit in der Informationsverarbeitung (BSI) empfohlen.[4]

Microsoft erhält persönliche Daten der Beschäftigten

Mit der Einführung von Windows 8.1 und Office 2013 stellt sich die Situation nunmehr so dar, dass Funktionen der vergleichbaren Vorgängerprodukte, die bisher ausschließlich lokal auf dem Rechner des Anwenders liefen, nun internetbasiert arbeiten und personenbezogene Daten der Anwender, hier also der Beschäftigten des Landes Niedersachsen, an Microsoft senden. Hierzu gehört beispielsweise die Hilfefunktion in sämtlichen Office-Programmen (vergl. http://www.microsoft.com/privacystatement/de-de/Office/default.aspx). In Anbetracht der Tatsache, dass Handbücher für Programme heute praktisch nicht mehr zur Verfügung stehen, sind die Beschäftigten gezwungen, die Übermittlung von Daten zur eigenen Person und zum eigenen Nutzerverhalten an Microsoft in Kauf zu nehmen, wenn mehr als nur die grundlegenden Funktionen dieser Produkte genutzt werden soll. Dies ist insbesondere deshalb ein erhebliches Datenschutzproblem, weil diese Übermittlung technisch unnötig ist, wie die Vorgängerprodukte erfolgreich belegt haben, und die Daten in ein Drittland übermittelt werden, dessen Datenschutzniveau trotz Safe-Harbor-Abkommens regelmäßig von mir kritisiert worden ist (siehe Beitrag auf Seite 113).

Fazit

Nach dieser erfolgreichen Produktumstellung bedarf es nun einer dringenden Fortentwicklung der IT-Sicherheitsarchitektur und der Sicherheitskonzepte unter Berücksichtigung der aktuellen Bedrohungslage und der datenschutzgerechten Anpassung der neuen Programmfunktionalitäten.

4 Vergl. https://www.bsi.bund.de/Sharfo_pdf.pdf?__blob=publicationFile sowie „BSI-Leitfaden Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen", veröffentlicht unter: https://netzpolitik.org/2015/trojaner-leitfaden-wir-veroeffentlichen-die-it-empfehlungen-die-das-bsi-aus-ruecksicht-auf-das-bka-geheim-hielt/)

Dataport und seine Kunden: Datenschutzbeauftragte weiter auf Abstimmungs- und Lösungskurs

Über Dataport, eine Anstalt des öffentlichen Rechts, und die Beratung und Kontrolle dieses IT-Dienstleisters durch die Datenschutzbehörden der Trägerländer Bremen, Hamburg, Schleswig-Holstein, Mecklenburg-Vorpommern, Sachsen-Anhalt (seit 2013 formal) und Niedersachsen hatte ich im letzten Tätigkeitsbericht erstmals umfänglich Ausführungen gemacht[1]. Die bewährte kooperative Zusammenarbeit der Datenschutzbeauftragten wurde auch im zurückliegenden Berichtszeitraum fortgesetzt.

In insgesamt sieben Sitzungen kam es 2013 und 2014 insbesondere zu folgenden Themen zu einem Informationsaustausch und gemeinsamen Stellungnahmen:

BYOD-Konzepte bislang nicht beherrschbar

Es wurden Szenarien und Lösungsansätze für Tablets und Smartphones im Betriebsmodus BYOD („Bring your own device") besprochen, da alle Länder diese Frage bewegt. Hier fehlte und fehlt es zunächst an überzeugenden Lösungen für die Rechtsprobleme. Dazu gehört, dass die Geräte Privateigentum des Bediensteten sind, jedoch das Erfordernis besteht, der IT-Sicherheits-Administration Regelungen und Eingriffe für die Sicherheitspolicy der Behörde (Sicherheitsdomäne) zuzugestehen. Das lässt sich nur mit Betriebsvereinbarungen regeln. BYOD ist allerdings als technisches Konzept mit seinen Komponenten grundsätzlich dazu geeignet, Verhalten und Arbeitsweise der Beschäftigten zu überwachen. Bei der Ausgestaltung der Vereinbarung und Nutzung hat daher der Personalrat ein Mitbestimmungsrecht.
Auch die Sicherheitsrisiken, die ein beliebig konfiguriertes Mobilgerät mit sich bringt, sind zahlreich. Die Hauptaspekte:

1. Die auf diesen Geräten installierten Betriebssysteme sind werksseitig aufgrund fehlender Rechte- und Rollenkonzepte und Administrationsrechte per se unsichere Plattformen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht bei Android davon aus[2], dass von App-Herstellern verursachte Veränderungen beziehungsweise Ergänzungen in der „Android-Landschaft" zu einer mittlerweile unüberschaubaren Vielzahl von angepassten Android-Versionen (Android-Fragmentierung) führen, die durch den Einsatz von Android auf verschiedenartigen Geräteklassen über klassische Smartphones hinaus, zum Beispiel Uhren, Unterhaltungssysteme und insbesondere Tablets, enorm an Komplexität gewinnen. Gefährdungen durch konzeptionelle Schwächen, systembedingte Mängel oder ausgenutzte Schwachstellen im Betriebssystem können mit den vom BSI empfohlenen Konfigurationen und Maßnahmen höchstens gemildert, jedoch nicht vollständig

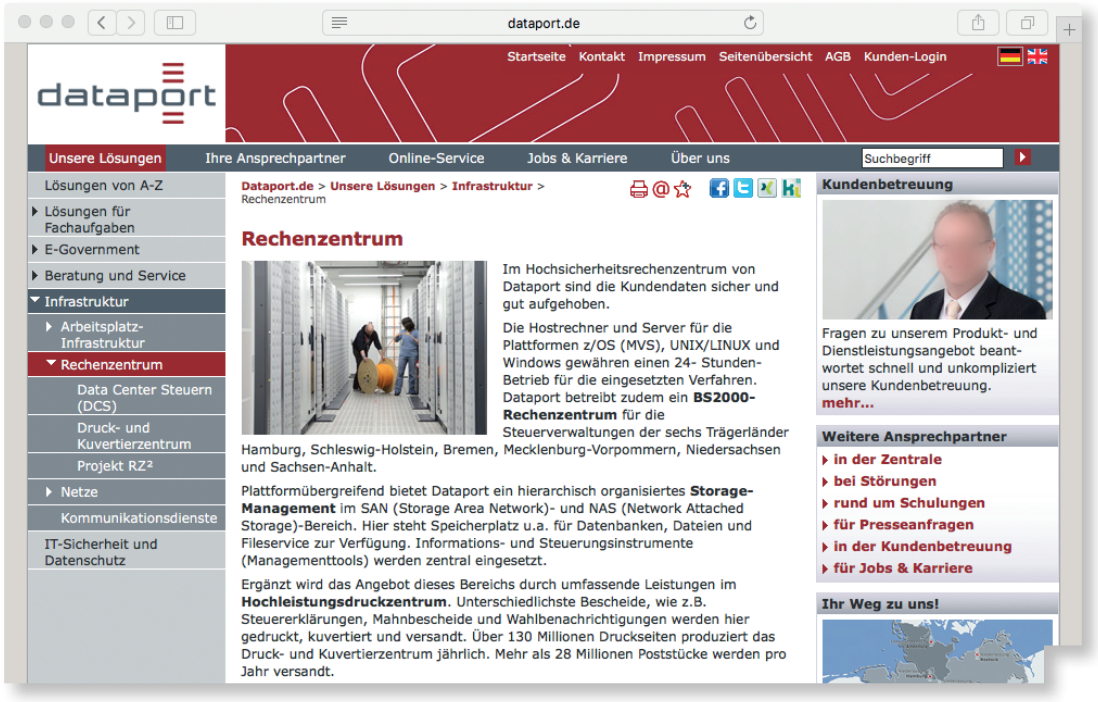
1 Kapitel „Gemeinsame norddeutsche Beratung und Prüfung: IT-Dienstleister Dataport", Seite 112 ff.
2 BSI-CS 109 | Version 1.00 vom 12. Mai 2015: Empfehlung: IT im Unternehmen, Android, Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/informationspool.html

beseitigt werden. Auch bei Apples iOS reichen laut BSI[3] aufgrund der Herkunft der Geräte aus dem Consumer-Bereich die Konfigurationseinstellungen nicht aus, um Geschäftsprozesse abzusichern, weshalb weitere Maßnahmen erforderlich sind.

2. Im BYOD-Betriebsmodus entfällt – nicht zuletzt wegen des Eigentumsverhältnisses – ein dienstlich betriebenes so genanntes Mobile Device Management (MDM). Das lässt sich aufgrund der Heterogenität auch nicht wirtschaftlich darstellen, weil jedes Gerät eine eigene Hard- und Softwarekonfiguration aufweist und keine der erforderlichen einheitlichen Handhabungen möglich sind. Eine Administrationsumgebung mit Fachpersonal ist auch deshalb zwingend, weil nur dort personenbezogene Daten schutzbedarfs- und risikogerecht systemseitig geschützt werden können und sicherheitsrelevante Hard- und Softwareeinstellungen mit angemessenen Schutzmaßnahmen vorgenommen und Angriffe sachgerecht abgewehrt werden können.
3. Die Voreinstellungen in der Konfiguration sind werksseitig häufig nicht auf maximalen Schutz gestellt.
4. Die heutigen Geräteklassen bieten inzwischen neben Telefonie, Videokonferencing, Datentransfer, Internetbrowsing, Social-Media-Clients, GPS-Ortung, Funknetzortung, NFC-Funkchips, lokaler Datenverarbeitung, Kontaktedaten, Fotografie, Videografie, Bildspeicher, Gesundheitsdaten, E-Mail-, Messenger-/Chat-Kommunikation und zahlreichen physischen Sensoren eine Vielzahl an Angriffsvektoren und Abhörmöglichkeiten, die zudem in Kombination miteinander potentiellen Angreifern zur Verfügung stehen.
5. Da im privaten Umfeld des Gerätes der Eigentümer beliebige der millionenfach verfügbaren Apps installieren kann, sind Sicherheitslücken, Spionagefunktionen und Programmierschwachstellen eine tägliche und hochwahrscheinliche Angriffslücke gegen die personenbezogenen Daten auf dem Gerät.
6. Sicherheitsstandards, die bei den herkömmlichen IT-Systemen wie Notebooks und Desktop-PC serienmäßig installiert sind, wie beispielsweise Firewalls (zur Portkontrolle), Malwareschutz (gegen Trojaner und Viren), fehlen dort regelmäßig. Eine solche Nachrüstung kann gerätebedingt nicht immer verwirklicht werden.
7. Die wenigsten marktgängigen Geräte ermöglichen im gemischten Betrieb des BYOD-Konzeptes eine konsequente Trennung zwischen privater und dienstlicher Datenhaltung; in der Konsequenz kann es zu einer Durchmischung von Daten und damit zum Verlust von Vertraulichkeit und Integrität kommen.
8. Eine Kontrolle darüber, ob Daten unzulässig über Verbindungen oder Speicherchips auf weitere Geräte transferiert werden, kann nicht sichergestellt werden.

Der Erfahrungsaustausch der Datenschutzbeauftragten zeigte, dass es noch keine befriedigende Strategie gibt, wie mit den Risiken rechtskonform umgegangen werden kann, ohne ein gehärtetes und speziell abgesichertes dienstliches Gerät einzusetzen.
Schwierigkeiten bereiten unter Umständen auch die Profilkennungen (Android: Google-ID, Apple: iOS-ID, Windows-LifeID) im Zusammenspiel mit den jeweiligen Appstores und den App-Zuordnungen. Apple bietet keine Hosting-Möglichkeit für einen eigenen Playstore.
Ein Bundesland beabsichtigte im Berichtszeitraum, zu prüfen, ob mit dem Produkt Excitor DME[4] aus Dänemark die Einbindung privater Smartphones ermöglicht werden kann. Dabei kommen dienstliche und private Endgeräte mit den Betriebssystemen iOS und Android zum Einsatz. Mit Excitor DME lässt sich ein so genanntes Enterprise Mobility Management (EMM) kombiniert betreiben und Secure-

3 BSI-CS 074 | Version 1.10 vom 26. Mai 2015, Empfehlung: IT im Unternehmen, iOS, Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit, a.a.O.
4 Excitor: https://www.excitor.com/solutions



mobile-container als abgeschottete Datenbereiche für E-Mails, Kontakte, Kalender, Zugang in das behördliche Intranet und Applications realisieren. Die dortige Entscheidung zum Betrieb existiert bereits seit 2012. Im Oktober 2014 stand noch eine Vorabkontrolle aus, obwohl bereits 1.100 Android-Geräte und 400 iOS-Geräte im Betrieb waren.

Ein weiteres Problem besteht darin, dass der Digitale Windows Rechte-Managementservice (DRM-System; Windows Rights Management Services, RMS) mit Verschlüsselung die Zustellung von Mails auf Mobile Devices mit hohem Schutzbedarf verhindert. Es bestand Einigkeit unter den Aufsichtsbehörden, dass mobile Endgeräte, mit denen dienstliche Aufgaben erledigt werden sollen, erheblich mehr Aufwand für systematische Schutzmaßnahmen erfordern, als dies in vielen Anwendungsfällen Realität ist.

Allgemein muss nach meiner Überzeugung jeder Lösungsansatz bereits ein Grundproblem lösen können: Bei den zahlreichen denkbaren Einsatzszenarien in der Landesverwaltung ist stets damit zu rechnen, dass bestimmte personenbezogenen Daten einen hohen oder sehr hohen Schutzbedarf aufweisen können. Angesichts der hohen Zahl teils kritischer Risiken ist die Beherrschbarkeit für die Integrität und Vertraulichkeit der Daten und der Verarbeitungsprozesse im BYOD-Betriebskonzept in Frage zu stellen. Nach meiner Auffassung ist es daher unzulässig.

Unlösbare Verkettungen von Abhängigkeiten

Dataport hegte aus betriebswirtschaftlichen Gründen die Vorstellung, länderübergreifend eine einzige Domain mit einem einzigen Verzeichnisdienst (hier: Active Directory, AD, der Microsoft Windows Server Umgebung) zu konzipieren, die damit sechs Bundesländer einbinden könnte. Dieser Planungsansatz traf auf große Skepsis der Datenschutzbehörden. Die fehlende Trennung zwischen den Ländern führt

nach meiner Überzeugung zu unlösbaren Verkettungen von Abhängigkeiten und hätte unvorhersehbare Folgewirkungen. Nach den Vorgaben der Orientierungshilfe Mandantenfähigkeit[5] wäre damit zu rechnen, dass eine Mandantentrennung nicht datenschutzkonform darstellbar wäre.
Die LfDI Bremen hat der Senatorin für Finanzen schriftlich am 4. Oktober 2013 mitgeteilt, dass es für ein gemeinsames AD an einer Rechtsgrundlage fehle. Diese Haltung nimmt auch der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) ein. Zwischenzeitlich stand die Frage im Raum, statt einer gemeinsamen Domain einen gemeinsamen übergeordneten Forest, also einen Verbund mehrerer zusammengehöriger Domains als Gesamtstruktur zu erstellen. Die maßgeblichen Informationen der darin enthaltenen Domains wären dann zum Abruf zentral im globalen Katalog verfügbar.
Im Oktober war dann von einer schriftlichen Mitteilung von der Dataport-Geschäftsführung an Bremen zu erfahren, es werde nunmehr doch ein zentrales länderübergreifendes AD geplant. Da hierfür eine Rechtsgrundlage fehlt, halten die Datenschutzbeauftragten diese Planung für problematisch.
Es wurden zahlreiche weitere Themen erörtert, die zwar nur bestimmte Länder betrafen, aber im Wege des beratenden Erfahrungs- und Bewertungsaustausches für alle Datenschutzbehörden relevant waren. Es seien hier einige Themen (nicht abschließend) genannt:

Keine Mandantentrennung bei Netviewer

Netviewer ist eine Software, mit der Unternehmen und Behörden Chats, Videokonferenzen und Desktop-Sharing realisieren können. Sie wird als Online-Support-Tool bei Finanzbehörden (nicht Niedersachsen) für den Helpdesk und die Fernadministration und bei Dataport intern bereits eingesetzt. Kritisch wurde hier gesehen, dass

- eine Videoprotokollierung für alle Sessions möglich ist und auf einem Server gespeichert wird, ohne dass eine Beschränkung der Aufzeichnung auf bestehende Bereiche möglich wäre,
- das Tool zur Unterstützung des Helpdesks bei Fachverfahren eingesetzt wird, in denen personenbezogene Daten verarbeitet werden (hier sind frühestmögliche unverzügliche Löschungen der Protokolle erforderlich, sobald die Daten objektiv nicht mehr benötigt werden),
- keine Mandantentrennung bei der Protokollierung für die verschiedenen Dienststellen und Bundesländer möglich ist,
- es Bestrebungen gibt, auf eine Datenverschlüsselung auf dem Server zu verzichten, weil administrative Tätigkeiten videoprotokolliert werden und damit eine Verfolgung möglich ist.

Alle kritischen Bewertungen wurden gegenüber Dataport und den betroffenen öffentlichen Stellen als Kunden bekannt gegeben.

Dataport-Rechenzentrum RZ²: Fragen und Zweifel

- Mehrfach gab es unterschiedliche Auffassungen zwischen den Datenschutzbehörden und Dataport über die Weitergabe von Dataport-IT-Sicherheitsdokumentationen an die beteiligten Kundenländer.

5 Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit – des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 1.0 vom 11. Oktober 2012, auf meiner Website www.lfd.niedersachsen.de unter Technik und Organisation > Orientierungshilfen und Handlungsempfehlungen > Mandantenfähigkeit; Deeplink: http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=31646&article_id=109520&_psmand=48

- Bei der Bereitstellung von Dokumentationen für die Datenschutzbehörden reicht es nach unserer Auffassung nicht aus, nur die Variante für andere Länder oder Massendokumente zu überreichen, wenn es um einzelne Prüfaspekte geht und auf Fragen Einzelantworten und gezielte Auszüge zu erwarten sind.
- Es kamen Zweifel an der Mandantenfähigkeit bestimmter Strukturen im Sinne der genannten Orientierungshilfe auf.
- Unklar blieb einige Zeit, wie es sich mit den Eigentumsverhältnissen der von Dataport gemieteten RZ-Serverräume verhält, was grundsätzliche Konsequenzen für die Subunternehmerschaft und die Betriebsverantwortlichkeiten hätte. Der Vermieter ist offenbar für Grundstück, Gebäude und Infrastruktur (OSI-Schicht 2) verantwortlich, während Dataport Mieterin ist. Unklar ist, ob dadurch ein Auftrags-Datenverarbeitungsvertrag geschlossen wurde oder nur ein Mietvertrag mit Betriebszusicherungen. Je nach Variante ergeben sich unterschiedliche Konsequenzen und Auswirkung auf die Datenschutz- und Informationssicherheitsprozesse, Zuständigkeiten und Verantwortlichkeiten. So bleibt auch offen, wie beispielsweise ein geordneter Shutdown der Systeme und Verfahren erfolgen kann.

E-Mailverkehr bei Dataport nach altem Standard

Im Oktober 2014 war aus der Dataport-Geschäftsleitung zu erfahren, dass dort noch keine Umstellung auf die sichere STARTTLS-Verbindungsverschlüsselung[6] erfolgt ist, obwohl dies vom HmbBfDI seit August 2014 gefordert worden war. Damit erfolgte der E-Mailverkehr bei Dataport noch immer nicht nach dem aktuellen Sicherheitsstandard. Das entspricht auch nicht der bereits im März 2014 erfolgten Entschließung der DSK[7] und ist aus Sicht der Datenschutzbeauftragten nicht hinnehmbar. Abgesehen von der Verbindungsverschlüsselung ist die Ende-zu-Ende-Verschlüsselung die entscheidende Forderung für sichere Kommunikation der Inhalte.

Fazit

Insgesamt hat es sich bewährt, dass sich die Datenschutzbeauftragten der Dataport-Trägerländer regelmäßig fachlich austauschen und damit möglichst abgestimmte Auffassungen gegenüber den nutzenden Ländern und gegenüber dem IT-Dienstleister Dataport abgeben. Es entsteht damit auch ein Mehrwert, weil praktische Erkenntnisse und Bewertungen zeitnah in den Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder einfließen.

6 STARTTLS-Spezifikation gemäß RFC 3207: https://tools.ietf.org/html/rfc3207

7 „Gewährleistung der Menschenrechte bei der elektronischen Kommunikation", Entschließung der 87. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März 2014 in Hamburg; http://www.lfd.niedersachsen.de/download/85979

Probleme mit der Mandantenfähigkeit: Projekt „Cloud-E-Mail“ ohne Niedersachsen

In meinem XXI. Tätigkeitsbericht hatte ich bereits ausführlich über die Erfordernisse berichtet, datenschutzkonforme Ausgestaltungen von IT-Verfahren im öffentlichen wie im nicht-öffentlichen Bereich zu gewährleisten, die für mehrere Mandanten – das sind Kunden, Organisationen oder einzelne verantwortliche Bereiche, die personenbezogene Daten verarbeiten – ausgelegt sind. Laufen also Verfahren gleicher Art für mehrere Mandanten auf denselben IT-Systemen, so sind technisch-organisatorische Schutzmaßnahmen zur Sicherstellung der Integrität und Vertraulichkeit sowie zum Trennungsgebot und zur Nichtverkettbarkeit jedes einzelnen Mandanten zu treffen. Dafür hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) 2012 eine Orientierungshilfe entwickelt[1].

Ein Anwendungsfeld der Mandantenfähigkeit ergab sich im Zusammenhang mit dem Projekt „Cloud-E-Mail“, das als Koordinierungsprojekt des IT-Planungsrates des Bundes und der Länder (IT-PLR-BL) initiiert worden war. Mit dem Projekt wird das Ziel verfolgt, beim Betrieb von gängigen Kommunikationslösungen wie dem Softwareprodukt Microsoft Exchange Synergieeffekte zu erzielen und Kosten für alle beteiligten Kundenbereiche für den Betrieb der Dienste E-Mail, Kalender, Kontakte und Aufgaben zu reduzieren. Gemeinsame Infrastrukturen für die IT-Nutzung der öffentlichen Verwaltung herbeizuführen, ist als eine der Kernaufgaben des IT-Planungsrates des Bundes und der Länder definiert.

Machbarkeitsanalyse in Auftrag gegeben

Der IT-PLR-BL hatte für dieses Projekt die Erstellung einer Machbarkeitsanalyse für die Umsetzbarkeit eines Cloud-E-Mail-Dienstes in der öffentlichen Verwaltung in Auftrag gegeben. Nach einer von der Finanzbehörde der Freien und Hansestadt Hamburg im Zusammenwirken mit Dataport (einer Anstalt des öffentlichen Rechtes, die im Übrigen auch von Niedersachsen mitgetragen wird) durchgeführten Analyse vom 12. September 2012[2] ist dies nur bei Ausgliederung an einen Dienstleister oder bei der Einbindung zusätzlicher Nutzer möglich. Damit würden folglich mehrere Kundenbereiche, also Mandanten, in einem gemeinsamen Anwendungsumfeld betrieben werden. Zugriffe etwa auf Kalender über Mandantengrenzen hinweg wären dabei eine erwünschte Option.
Die Prüfung führte unter anderem zu dem Ergebnis, dass durch die Mandantenfähigkeit jeder Teilnehmer seine bisherigen Vorgaben an das eigene E-Mail-System auch künftig in einem gemeinsamen System umsetzen könne. Inwieweit ein Teilnehmer nach seinen jeweiligen rechtlichen Vorgaben in der Lage sei, einen Dienstleister in der öffentlichen Verwaltung zu beauftragen, sei jedoch nicht Gegenstand der Machbarkeitsstudie. Dies müsse jeder Teilnehmer in seinem Zuständigkeitsbereich prüfen.

1 Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit – des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Version 1.0 vom 11. Oktober 2012; auf meiner Website www.lfd.niedersachsen.de unter > Navigation > Technik und Organisation > Orientierungshilfen und Handlungsempfehlungen > Mandantenfähigkeit; Deeplink: http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=31646&article_id=109520&_psmand=48

2 Machbarkeitsanalyse eines nationalen Exchange-Dienstes „Cloud-E-Mail-Dienst“, Stand: 12. September 2012, Version 1.4

Orientierungshilfe nicht hinreichend beachtet

Die Analyse geht davon aus, dass existierende Anforderungen an Datenschutz und Informationssicherheit nicht harmonisiert werden müssten, da bestehende Konfigurationsmöglichkeiten innerhalb der Mandanten auch bei Nutzung des Cloud-E-Mail-Dienstes erhalten blieben. Diese Einschätzung betrachte ich als kritisch, weil nicht alle Aspekte der datenschutzrechtlich erforderlichen Trennung von Daten, Systemen und Prozessen durchgesetzt werden können, wenn übergreifende Implementierungen und Konfigurationen faktische Abweichungen beinhalten. Die von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder verabschiedete Orientierungshilfe Mandantenfähigkeit wurde offensichtlich nicht hinreichend beachtet.
Der IT-Planungsrat des Bundes und der Länder hatte in seiner 9. Sitzung im Herbst 2012[3] die genannte Machbarkeitsanalyse für die Umsetzbarkeit eines Cloud-E-Mail-Dienstes in der öffentlichen Verwaltung zur Kenntnis genommen und beschlossen, dass sich bis 31. Januar 2013 der Bund und die Länder jeweils entscheiden sollten, ob sie an diesem gemeinsamen Dienst grundsätzlich Interesse haben. Auf der Grundlage der Rückmeldungen (sieben Länder zeigten Interesse) sollte die Projektgruppe den Moderationsprozess zur Klärung der weiteren Vorgehensweise übernehmen und auf der 10. Sitzung des IT-Planungsrats über die Ergebnisse berichten. In dieser Sitzung im März 2013 beschloss der IT-PLR-BL, dass die interessierten Mitglieder des IT-Planungsrats im Rahmen des Koordinierungsprojekts „Cloud-E-Mail" Umsetzungen vorbereiten und dem IT-Planungsrat zu gegebener Zeit berichten werden.[4]

Niedersachsen macht nicht mit

Nach einem Informationsaustausch und fachlicher Beratung des Arbeitskreises Technische und organisatorische Datenschutzfragen (AK Technik) der Konferenz der Datenschutzbeauftragten von Bund und Ländern im Februar 2013 ergaben sich für mich mehrere Faktoren, die bei diesem Projekt datenschutzrechtlich schwierig zu lösen sind:

- Insbesondere würde ein zentraler Exchange-Cluster auch einen zentralen Verzeichnisdienst, hier ein Microsoft basierendes zentrales Active Directory (AD), nahelegen, das jedoch weitere datenschutzrechtliche Probleme verursachen würde. Dataport hat Anfang 2013 eine Vorstudie dazu durchgeführt, um zu ermitteln, ob Lösungen mit mehreren AD oder mit einem zentralen AD möglich sind.
- Bei mangelnder oder mangelhafter Mandantenfähigkeit der Exchange-Lösung wäre es erforderlich, die damit verarbeiteten Mails zu verschlüsseln, um das Schutzziel der Vertraulichkeit zu erfüllen. Daraus würden sich jedoch zusätzliche Kosten statt der erwünschten Einsparmöglichkeiten ergeben.

Erfreulicherweise verwarfen der IT-Planungsrat Niedersachsen und das Niedersächsische Ministerium für Inneres und Sport eine Teilnahme an diesem Verfahren, weil es weder als wirtschaftlich noch sicherheitstechnisch beherrschbar angesehen wurde.

3 Sitzungsniederschrift zur 9. Sitzung des IT-Planungsrates des Bundes und der Länder: http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/9._Sitzung/Entscheidungsniederschrift_ITPLR_09.html?nn=1852114

4 IT-Planungsrat des Bundes und der Länder, Ergebnisse: http://www.it-planungsrat.de/DE/Entscheidungen/2013/10_Sitzung/10_Sitzung_node.html#doc3348826bodyText11

E-Mailverkehr in der Justizverwaltung: Ende-zu-Ende-Verschlüsselung zwingend nötig

Nachdem das Niedersächsische Justizministerium bereits innerhalb seines nachgeordneten Bereichs den Versand von hochsensiblen Daten im Jahre 2012 per E-Mail freigegeben hatte, erfolgte im Jahre 2013 eine Ausweitung unter Einbeziehung des Polizeibereichs. Die nötigen Unterlagen zum Nachweis eines ausreichenden Schutzes dieser Daten lagen mir auch im Frühjahr 2015 noch nicht vor.

Die Vorzüge einer schnellen Kommunikation per E-Mail sind unbestreitbar und auch aus der Verwaltung nicht mehr wegzudenken. Aus diesem Grunde wird für viele Bereiche die Umstellung von anderweitigem Datenaustausch auf E-Mail erwogen und – soweit rechtlich möglich – auch dort umgesetzt, wo Bedenken hinsichtlich der Sicherheit und Vertraulichkeit bisher einer Kommunikation per E-Mail entgegenstanden. Im Bereich der Justizverwaltung betrifft dies den Versand besonders vertraulicher personenbezogener Daten. Um die Risiken abschätzen und die notwendigen Sicherungsmaßnahmen treffen zu können, werden die Daten zunächst nach ihrer Sensibilität anhand des Schutzstufenkonzeptes[1] kategorisiert. Dabei reichen die Schutzstufen von A (frei zugänglich) bis E (Gefahr für Leib und Leben).
Seit dem Jahr 2012 versenden Staatsanwaltschaften und Gerichte auch Daten der Schutzstufen D (existenzgefährdend) und E (Gefahr für Leib und Leben) innerhalb des Geschäftsbereichs des Justizministeriums per E-Mail. Begründet wird dies mit einer Umstellung der IT-Technik: Der ressortinterne Mailverkehr wird zum einen nicht mehr wie bisher über landesweit erreichbare Rechner des landeseigenen zentralen IT-Dienstleisters, sondern direkt geführt. Außerdem wird der Mailverkehr zwischen den beteiligten Mailservern verschlüsselt (Transportverschlüsselung). Im Jahre 2013 wurde der Nachrichtenaustausch von Daten der Schutzstufen D und E seitens der Justiz um den Bereich der Polizei erweitert.

Technische Risiken, fehlerhafte Software

Nach herrschender Auffassung der Datenschutzbehörden sind die Risiken, die bei der Verarbeitung von personenbezogenen Daten der Schutzstufe E auftreten, bei vernetzten Arbeitsplatzrechnern nur schwer beherrschbar. Dies gilt in besonderem Maße, wenn diese über das lokale Netzwerk der Dienststelle an das Landesnetz mit vielen tausend angeschlossenen Rechnern angebunden werden. Verschärfend kommt hinzu, dass die Rechner über das Landesnetz auch über einen Internetzugang für SMTP und HTTP verfügen. Aufgrund der Komplexität der heute eingesetzten Software ist diese von einer Fehlerfreiheit weit entfernt, was nicht zuletzt durch Updates belegt wird, die von den Herstellern regelmäßig bereitgestellt werden. Besonders problematisch sind Sicherheitslücken, die schon ausgenutzt werden, bevor die Hersteller entsprechende Sicherheitsupdates zur Verfügung stellen (so genannte Zero-Day-Exploits). Gleiches gilt für Schadprogramme, die von den Virenscannern zum Zeitpunkt ihres Auftauchens noch nicht erkannt werden.

Reine Transportverschlüsselung unzureichend

Hieraus ergibt sich das Risiko, dass durch Ausnutzung entsprechender Schwachstellen vertrauliche Daten sogar außerhalb des Landesnetzes Unberechtigten zur Kenntnis gelangen können. Die Eintrittswahrscheinlichkeit ist zwar als eher gering einzuschätzen, der Schaden im Eintrittsfall jedoch so hoch, dass

1 vgl. http://www.lfd.niedersachsen.de/download/52033/Schutzstufenkonzept_LfD_Niedersachsen_.pdf

dies zumindest bei Daten der Schutzstufe E als ein nicht vertretbares Risiko anzusehen ist. Hinzu kommt, dass bei einer reinen Transportverschlüsselung an den Arbeitsplatzrechnern sowie den an der Kommunikation beteiligten Mailservern eine unbefugte Kenntnisnahme grundsätzlich möglich ist, da die Daten dort unverschlüsselt vorliegen. Des Weiteren besteht bei Schwächen der Transportverschlüsselung die Gefahr eines Man-in-the-Middle-Angriffs während der Übermittlung. Darüber hinaus muss die Möglichkeit der Fehlbedienung des Mailprogrammes berücksichtigt werden, die dazu führt, dass die Daten versehentlich einem Dritten zur Kenntnis gelangen. Der Einsatz einer Ende-zu-Ende-Verschlüsselung ist daher als notwendiges, aber nicht hinreichendes Kriterium zwingend zu fordern.

Verfahrensbeschreibung und Vorabkontrolle nicht vorgelegt

Gerade bei derart sensiblen Daten kommt der Erstellung einer Verfahrensbeschreibung sowie der Vorabkontrolle nach § 7 Abs. 3 Niedersächsisches Datenschutzgesetz (NDSG) eine besondere Bedeutung zu. Gerade letztere soll der verantwortlichen Stelle dazu dienen, vor Aufnahme eines Verfahrens eventuelle nicht vertretbare Gefahren zu erkennen, zu beseitigen und dies zu dokumentieren.
Bis zum Frühjahr 2015 hat mir die Justiz diese Unterlagen – auch auf Nachfrage – nicht vorgelegt.
Bemerkenswert ist, dass seitens der Zentralen Polizeidirektion (ZPD) eine Vorabkontrolle zum Mailverkehr innerhalb des Netzes der Polizei und zum Austausch mit Justizbehörden vorgelegt wurde, in der die ZPD zu dem Ergebnis gelangt, dass „von einer Verarbeitung von Daten der Schutzstufe E […] aufgrund des verbleibenden Restrisikos aus datenschutzrechtlicher Sicht dringend abzuraten [ist] …".
Da zumindest das Netz der Polizei keinen hinreichenden Schutz für Daten der Schutzstufe E bietet, ist davon auszugehen, dass eine Mailkommunikation zwischen Justiz und Polizei unter datenschutzrechtlichen Gesichtspunkten als rechtswidrig zu betrachten ist und die noch fehlende Vorabkontrolle der Justiz zum gleichen Ergebnis kommen muss.

Strafverfahren eventuell gefährdet

Der Staat und seine Organe sind nicht nur in besonderem Maße zur Wahrung der Rechtmäßigkeit ihres Handelns verpflichtet, sondern haben darüber hinaus die ihnen anvertrauten Daten ausreichend zu schützen. Insbesondere haben sie beim Einsatz informationstechnischer Systeme ihr besonderes Augenmerk auf die Schutzziele Vertraulichkeit und Integrität zu richten, die nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfG, 1 BvR 370/07 vom 27. Februar 2008) als Bestandteile des allgemeinen Persönlichkeitsrechtes (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) gelten. Auch wenn es keine höheren Schutzgüter als Unversehrtheit, Leben und Freiheit gibt, kommt bei einer Missachtung datenschutzrechtlicher Anforderungen gerade im Bereich der Justiz ein weiteres schwerwiegendes Risiko hinzu: Wenn Zeugen oder andere Betroffene wie zum Beispiel V-Leute im Bereich von organisierter Kriminalität und Terrorismus dem Schutz ihrer Daten durch Polizei und Justiz nicht mehr voll vertrauen, besteht die Gefahr, dass diese Personen für ein Strafverfahren nicht mehr zur Verfügung stehen und schwerwiegende Verbrechen im ungünstigsten Fall ungeahndet bleiben. Daher bedeutet die Einhaltung datenschutzrechtlicher Vorschriften nicht nur den Schutz eines wesentlichen Grundrechtes. Sie ist vielmehr zwingend erforderlich für ein funktionierendes Justizsystem.

Elementare Gewährleistungsziele: Das Standard-Datenschutzmodell nimmt Konturen an

In meinem XXI. Tätigkeitsbericht 2011-2012 hatte ich ausführlich über die konkrete Weiterentwicklung berichtet, die das Standard-Datenschutzmodell (SDM)[1] erfahren hat. Als Folge der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) vom 18. März 2010 zu einem Eckpunktepapier für eine Modernisierung des Datenschutzrechtes[2] war es notwendig geworden, das Modell der sechs abschließenden elementaren Schutzziele um eine vollständige Beschreibung eines Referenzschutzmaßnahmen-Modells zu ergänzen.

Ziel war es aus fachlicher Sicht des technischen Datenschutzes nicht, lediglich eine akademische Übung zu absolvieren, sondern eine schlüssige Methodik für den praktisch umsetzbaren Grundrechtsschutz und ein praxistaugliches modellhaftes Werkzeug zu entwickeln. Dieses ist Mittler zwischen datenschutzrechtlichen Grundsätzen und konkreten Rechtsnormen einerseits und der Umsetzung bei der Feststellung der Anforderungen an angemessene technisch-organisatorische Maßnahmen (§ 9 BDSG oder § 7 NDSG) andererseits. Durch vollständige Beschreibungen und die Systematisierung sollte nun durch eine ergänzende Definition von generischen Schutzzielen und eine Verfeinerung der abzuleitenden konkreten Schutzmaßnahmen ein nächster Schritt erfolgen. Dies war die Fortsetzung auf dem Weg zu einer Methodik, die für den Alltag der Modellierung von IT-Systemen sowie bei der Revision, Auditierung und Kontrolle bestehender IT-Verfahren benötigt wird.

Die Ideen und ihre Folgen: SDM-Handbuch und Referenzmaßnahmen

Ein erstes Positionspapier des Unabhängigen Landeszentrums für Datenschutz (ULD) Schleswig-Holstein vom Januar 2013 beriet der Arbeitskreis Technische und organisatorische Datenschutzfragen (AK Technik) der DSK im Februar 2013. Die Standardmethodik sollte neben dem IT-Grundschutz etabliert werden. Nach eingehender Erörterung wurde beschlossen, im Modell die Datensparsamkeit nicht dem Schutzziel Nichtverkettbarkeit unterzuordnen und in das Modell die Europa-Perspektive (Entwurf der EU-Datenschutzgrundverordnung) aufzunehmen.
Damit die Arbeit fortgesetzt werden konnte, setzte der AK Technik eine Unterarbeitsgruppe SDM (UAGSDM) mit juristischem und technischem Sachverstand ein, die an der Systematisierung und Formulierung des SDM-Handbuches weiterarbeitete. Die 85. DSK im März 2013 nahm das SDM-Handbuch zur Kenntnis und erteilte der UAGSDM den Auftrag zur Weiterentwicklung und einer eingehenden Ausarbeitung des Nachweises der rechtlichen Deckung der Schutzziele.

1 XXI. Tätigkeitsbericht 2011-2012, Seite 100ff: „Schutzziele statt Kontrollziele: Neues Referenzmodell für technische und organisatorische Datenschutzmaßnahmen“

2 „Ein modernes Datenschutzrecht für das 21. Jahrhundert – Eckpunkte“, verabschiedet von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. März 2010, Kapitel 3 „Technischer und organisatorischer Datenschutz“: www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.html?nn=408908

In den Sitzungen der UAGSDM wurden 2013 und 2014 folgende Ergebnisse erzielt:

- Entwicklung des SDM-Handbuches einschließlich des Betriebskonzeptes zur kontrollierten Fortschreibung des SDM und (generischer) Referenz-Schutzmaßnahmen.
- Detaillierte Erarbeitung des Nachweises der rechtlichen Deckung der Schutzziele. Mit einer Zuordnungstabelle wird die Vereinbarkeit der Schutzziele mit dem BDSG und den Landesdatenschutzgesetzen subsumiert.
- Die Schutzziele werden in Gewährleistungsziele umbenannt, um nicht in Konflikt mit den Ländern zu geraten, deren Datenschutzgesetze bereits Schutzziele ausweisen.
- Ausweisung von technisch-organisatorischen Standardmaßnahmen nur für den Schutzbedarf „normal“ und „hoch“. Für den Schutzbedarf „sehr hoch“ sind keine Standards vorgesehen.
- Unterscheidung nun von vier Verfahrenskomponenten: Daten, IT-Systeme (Hardware und Software), organisatorische Prozesse (sozial-funktionale Regelungen von Abläufen) und technische Prozesse (technisch-funktionale Abläufe).
- Der Bezug zum IT-Grundschutz-Maßnahmenkatalog soll aufrecht erhalten bleiben, jedoch unter Berücksichtigung der Betroffenenperspektive.

Das SDM-Handbuch (Version 0.8) wurde im Oktober 2014 von der DSK abgenommen. Sie erteilte der UAGSDM zwei Aufträge:

- Englisch-Übersetzung des Handbuchs, vornehmlich mit Bezug zu Europa (für die Art.-29-Gruppe),
- Entwicklung eines Referenzkatalogs für Standard-Maßnahmen bis zur DSK-Herbstsitzung 2015.

Meine Behörde war seitens des Technikreferates neben einigen anderen Datenschutzbehörden an allen Arbeitsgruppenphasen seit 2008 beteiligt und wirkte auch 2013 und 2014 an den Arbeiten zum SDM und dem Referenzmaßnahmenkatalog mit.

Ausblick

Geplant ist, im April 2015 einen Workshop des AK Technik durchzuführen, um im Diskurs zwischen Juristen und Informatikern der Datenschutzbeauftragten des Bundes und der Länder das grundrechtlich verankerte Datenschutzrecht abzusichern und die beabsichtigte systematische Transformation von der rechtlichen Basis zur praktischen Umsetzung durch technisch-organisatorische Maßnahmen abzustimmen.

Zur Erinnerung: Warum ein neues Standard-Datenschutzmodell?

Dem Datenschutz kommt wegen des Verfassungsranges der Persönlichkeitsrechte ein Vorrang gegenüber der Informationssicherheit zu. Dies kann in der Praxis angesichts immer komplexer werdender IT-Verfahren und unterschiedlichster und sehr schnell weiterentwickelter allgegenwärtiger Technologien jedoch nur erfolgreich durchgesetzt werden, wenn Datenschutzprüfungen methodisch zumindest auf dem gleichen Niveau stattfinden wie Prüfungen der Informationssicherheit nach den dafür etablierten Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) oder der ISO 27001.

Konzept war kein Zufallsprodukt

Im Jahre 2008 und 2009 haben Martin Rost und andere Mitarbeiter des ULD Schleswig-Holstein gemeinsam mit Prof. Andreas Pfitzmann (†) und Mitarbeitern weiterer LfD ein neues Datenschutzmodell erarbeitet. Einige grundlegende Überlegungen gehen auch auf das viel beachtete Gutachten im Auftrag des Bundesinnenministeriums im Jahr 2001[3] zurück. Es basiert auf

- den sechs elementaren Schutzzielen (neu: Gewährleistungsziele) Nichtverkettbarkeit, Intervenierbarkeit, Transparenz, Vertraulichkeit, Integrität und Verfügbarkeit,
- den drei Verfahrenskomponenten Daten, Systeme/IT-Infrastruktur und Prozesse sowie
- den drei Schutzklassen normal, hoch und sehr hoch.

Die drei letzten Schutzziele sind aus dem Grundschutz bekannt und wurden 2008 durch ein Urteil des Bundesverfassungsgerichts durch Nennung der Integritäts- und Vertraulichkeitserfordernisse zu einer festen Größe im Grundrechtsschutz. Der Staat hat fortan die Umsetzung der Schutzziele Vertraulichkeit und Integrität zu gewährleisten.

Auch die Verfahrenskomponenten sind bereits Bestandteil des IT-Grundschutzes. Der Datenschutzbezug ergibt sich jedoch nicht mehr nur aus den Daten, sondern auch aus den Verfahren. Die in ihrer Abstufung ebenfalls bereits bekannten Schutzklassen beziehen sich jedoch nicht mehr auf die Sicht einer Organisation, sondern werden aus dem Blickwinkel des Individuums betrachtet. In Analogie zur Grundschutzmethodik werden Standardmaßnahmen für jede Kombination aus Schutzziel, Verfahrenskomponente und Schutzklasse definiert und beschrieben. Erste Ansätze hierfür fanden sich in der Literatur. Der erforderliche Prozess zur Umsetzung des Modells kann in Anlehnung an die bewährte Grundschutzmethodik des BSI oder der ISO 27001 definiert werden.

Der Arbeitskreis Technische und organisatorische Datenschutzfragen (AK Technik) der Datenschutzbeauftragten des Bundes und der Länder verabschiedete 2009 schließlich den Zwischenbericht „ Empfehlungen für die Vereinheitlichung der Regelungen zum technischen und organisatorischen Datenschutz“ und legte diesen der DSK vor. Das darin beschriebene Konzept fand seinen Niederschlag in dem bereits erwähnten DSK-Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ vom 18. März 2010.

3 Alexander Roßnagel, Andreas Pfitzmann, Hansjürgen Garstka, Gutachten im Auftrag des Bundesministeriums des Innern, 2001: „Modernisierung des Datenschutzrechts“; Quelle: http://www.bfdi.bund.de/SharedDocs/VortraegeUndArbeitspapiere/2001GutachtenModernisierungDSRecht.pdf?__blob=publicationFile

Vernichtung von Datenträgern: Handlungsempfehlung baut Brücke zwischen Datenschutz und DIN 66399

Die Vernichtung von Datenträgern ist eine Möglichkeit, der datenschutzrechtlichen Verpflichtung zum Löschen von personenbezogenen Daten nachzukommen. Diese kann sich sowohl aus dem Bundesdatenschutzgesetz (§ 20 Abs. 2 und § 35 Abs. 2 BDSG) als auch aus dem Niedersächsischen Datenschutzgesetz (§ 17 Abs. 2 NDSG) oder anderen spezialgesetzlichen Regelungen (zum Beispiel § 84 Abs. 2 SGB X) ergeben.

Im Oktober 2012 veröffentlichte das Deutsche Institut für Normung die neue dreiteilige DIN 66399 mit dem Titel „Büro- und Datentechnik – Vernichtung von Datenträgern". Sie löste die alte Norm aus dem Jahr 1995 ab. Der damit für diesen Bereich neu definierte Stand der Technik gab dem Arbeitskreis Technische und organisatorische Datenschutzfragen (AK Technik) der Datenschutzbeauftragten des Bundes und der Länder Anlass zu prüfen, inwieweit eine ergänzende Orientierungshilfe erforderlich und geeignet sei, als „Transformationshilfe" für speziell datenschutzrechtliche Anforderungen zu dienen.
Zur Klassifizierung des Schutzbedarfes der zu vernichtenden Daten weist die DIN 66399 drei Schutzklassen auf: normaler, hoher und sehr hoher Schutzbedarf. Weiterhin werden sieben Sicherheitsstufen definiert, die den Grad der Wirksamkeit einer Vernichtung darstellen; je höher die Sicherheitsstufe, desto höher der Reproduktionsaufwand für einen mutmaßlichen Angreifer. Anschließend folgt die Empfehlung, Datenträger mit Daten bestimmter Schutzklassen nur nach bestimmten Sicherheitsstufen zu vernichten.

Ergänzende Hinweise

Sowohl bezüglich der Begriffsbestimmungen, als auch der getroffenen Zuordnung von Schutzklassen zu Sicherheitsstufen und einer damit letztendlich konsolidierten Risikobetrachtung, die sich naturgemäß eher an der Vorgehensweise der IT-Sicherheit als der des Datenschutzes orientiert, sah der AK Technik sinnvolle Anknüpfungspunkte für ergänzende Hinweise, welche die Sinnhaftigkeit und Logik der DIN jedoch keineswegs in Frage stellen sollten. So galt es unter anderem zum Ausdruck zu bringen, dass

- sich die Wahrung grundrechtsnormierter datenschutzrechtlicher Anforderungen nicht in jedem Falle mit rein wirtschaftlichen Erwägungen in Einklang bringen lässt,
- es spezialgesetzliche Regelungen erfordern könnte, im Rahmen der Schutzbedarfsklassifizierung die Zuordnung bestimmter Daten zu den Schutzklassen der DIN zu modifizieren (zum Beispiel Wahl einer höheren Schutzklasse, wenn das Verbot der Offenbarung von Geschäfts-, Betriebs-, Berufs- oder Amtsgeheimnissen im Sinne von § 203 StGB tangiert ist),
- im Zweifel aufgrund einer besonderen Risikobetrachtung des gesamten Vernichtungsprozesses im Einzelfall ebenfalls von der Sicherheitsstufenempfehlung der DIN abgewichen werden kann.

Im Vorfeld und im Nachgang von zwei AK-Sitzungsterminen wurde unter Mitwirkung meiner Behörde ein entsprechendes Arbeitspapier entwickelt, das ich Interessierten als Handlungsempfehlung meines Hauses zur Verfügung stelle.

Handlungsempfehlung zur Ermittlung des Schutzbedarfs personenbezogener Daten für den Prozess der Datenträgervernichtung: www.lfd.niedersachsen.de > Technik und Organisation > Orientierungshilfen > Vernichtung und Löschung

11. Datenschutzinstitut Niedersachsen

Fortbildungsbedarf nimmt weiter zu

Wie in den vergangenen Jahren fand auch im Berichtszeitraum für Beschäftige der öffentlichen Verwaltung eine Reihe von Veranstaltungen in dem zu meiner Behörde gehörenden Datenschutzinstitut Niedersachsen (DsIN) statt. Besonders nachgefragt war erneut die mehrtägige Seminarreihe „Basiswissen für behördliche Datenschutzbeauftragte".

Die aktuellen Konzepte des DsIN beruhen nach wie vor auf der Erkenntnis, dass die meisten Datenschutzverstöße in der Praxis nicht durch die gezielte Verletzung der Vorschriften verursacht werden, sondern überwiegend auf Unkenntnis der bestehenden Regelungen basieren, sofern es sich nicht um gezielte Angriffe unter Nutzung von Sicherheitslücken in Hard- und Software handelt. Der Schwerpunkt meiner Arbeit lag und liegt daher in der Sensibilisierung für datenschutzgerechte Vorgehensweisen. Die Teilnehmerinnen und Teilnehmer sollen in die Lage versetzt werden, als Multiplikatoren in ihrem Fachbereich das Datenschutzbewusstsein zu fördern.

Basiskurs stets ausgebucht

Traditionell am stärksten nachgefragt und stets ausgebucht ist der Kurs „Basiswissen für behördliche Datenschutzbeauftragte". In dieser viertägigen Veranstaltungsreihe werden die grundlegenden rechtlichen und technisch-organisatorischen Aspekte der Tätigkeit einer oder eines behördlichen Datenschutzbeauftragten dargestellt und an Hand praktischer Beispiele mit den Teilnehmenden durchgespielt.
Neben den genannten Seminarreihen werden jährlich Einzelveranstaltungen mit Schwerpunktthemen (Einführung in das Datenschutzrecht, Personaldatenschutz, Sozialdatenschutz, Datenschutz in Schulen sowie Themen aus dem technisch-organisatorischen Bereich) angeboten. Zusätzlich konnte im Berichtszeitraum ein weiteres Fortbildungsangebot realisiert werden, das sich vorrangig mit Web 2.0 und den sozialen Netzwerken (Social Media) und deren besonderen datenschutzrechtlichen sowie technischen Herausforderungen befasst.
Neben diesen Angeboten ist der Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der teilnehmerstärkste Kurs (siehe auch Seite 57 zum Thema „Netzwerkpflege"). Als zusätzliches Angebot wurden Inhouse-Veranstaltungen zum Thema „Einführung in das Datenschutzrecht" bei verschiedenen Kommunen, Schulen und im Bereich des Justizministeriums durchgeführt. In den Grundkursen werden die Grundlagen der komplexen Rechtsmaterie des Datenschutzes unter Berücksichtigung der besonderen Belange im Bereich der Kommunal- oder Landesverwaltung sowie der Fragestellungen aus der Arbeitspraxis vermittelt.

Informationstechnologie dominiert

Insbesondere der Basiswissenkurs für behördliche Datenschutzbeauftragte macht deutlich, wie sehr neben der juristischen Bewertung die Informationstechnologie die Datenschutzthemen inzwischen dominiert und deshalb ein hohes Maß an personellem Aufwand und Einsatz erforderlich ist. Allein für die zu vermittelnden technischen Inhalte entstanden im Berichtszeitraum 32 Tage Zeitaufwand. Bis Ende 2014 wurden diese Angebote von drei Mitarbeitern des Technikreferates, parallel zu deren Aufgaben der Eingabenbearbeitung, Beratung und Kontrolle, geleistet. Dabei wurden insgesamt 22 Veranstaltungstage realisiert; das entspricht einem Anteil von rund 36 Prozent des Gesamtvolumens der DsIN-Veranstaltungen.

Insgesamt konnten im Berichtszeitraum für rund 500 Personen 37 Schulungsangebote an 61 Tagen durchgeführt werden. Die Nachfrage nach weiteren Kursangeboten ist sehr hoch. Leider können nicht alle Schulungsanfragen bedient werden, da mir die personellen Ressourcen für zusätzliche Fortbildungsangebote aktuell nicht zur Verfügung stehen.

Mehr Angebote geplant

Aufgrund der vielen positiven Rückmeldungen zu unserem Kursangebot ist es mir ein großes Anliegen, das Schulungsangebot des Datenschutzinstituts im nächsten Berichtszeitraum weiter auszubauen und darüber hinaus neue Formate zu entwickeln, um auf diese Weise einen breiteren Personenkreis als bisher ansprechen zu können. Ich würde mich freuen, wenn die Landesregierung und der Landtag diesen Weg positiv begleiten und im notwendigen Umfang unterstützen.

Weitere Informationen: www.lfd.niedersachsen.de > Fortbildung/Service > Datenschutzinstitut Niedersachsen

12. Neue Aufgabe!?

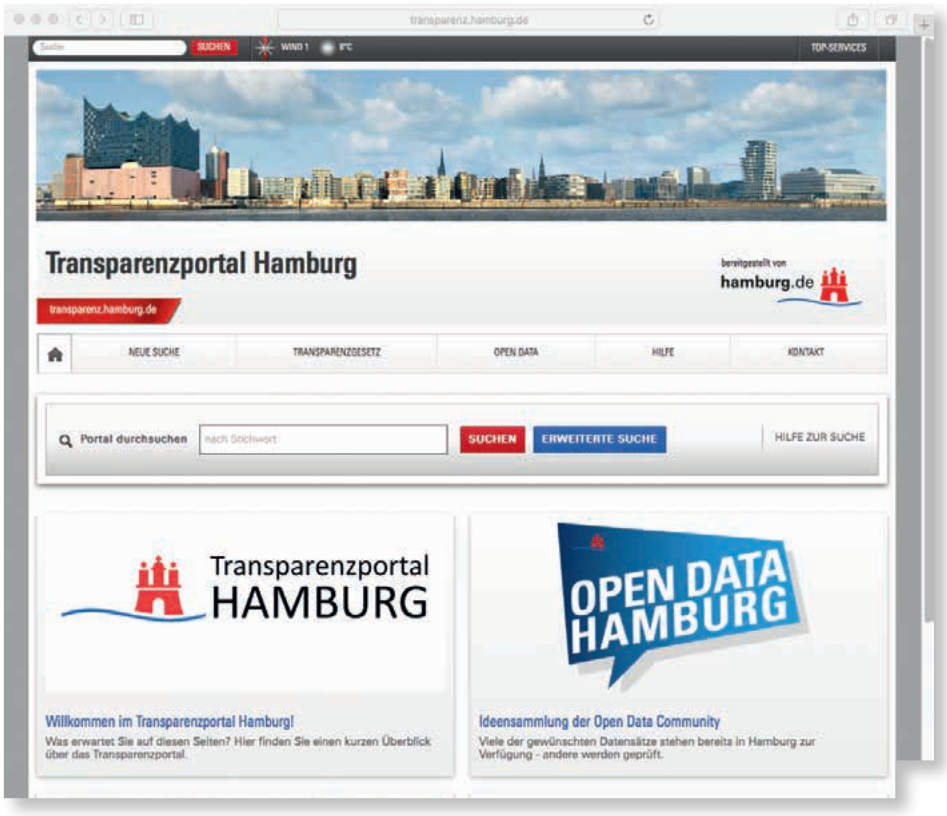
Ein Informationszugangs- und Transparenzgesetz für Niedersachsen

Mit dem brandenburgischen Akteneinsichts- und Informationszugangsgesetz wurde 1998 das bundesweit erste Landesinformationszugangsgesetz erlassen. Es folgten Berlin 1999, Schleswig-Holstein 2000 und Nordrhein-Westfalen im Jahre 2001. Aktuell sind in allen Bundesländern und dem Bund mit Ausnahme der Länder Baden-Württemberg, Bayern, Hessen, Sachsen und Niedersachsen Informationsfreiheitsgesetze (IFG) in Kraft. Diese Gesetze stellen ein Jedermannrecht dar, auf dessen Grundlage Bürgerinnen und Bürger, ohne eine Betroffenheit oder eine Begründung darlegen zu müssen, auf Antrag Zugang zu staatlichen Informationen erhalten können. Die meisten dieser Gesetze wurden inzwischen evaluiert und teilweise entsprechend der jeweiligen Erkenntnisse novelliert.

In der Gesamtschau bleibt festzustellen, dass einerseits die Befürchtungen, es entstünden gläserne Bürgerinnen und Bürger und eine durch Antragsflut gelähmte Verwaltung, bisher nicht eingetreten sind. Andererseits sind jedoch auch der Bekanntheitsgrad der Gesetze und die Zahl der Anträge hinter den Erwartungen zurückgeblieben. Auch in Niedersachsen gab es einige Ansätze, ein Informationsfreiheitsgesetz auf den Weg zu bringen, die jedoch bislang nicht erfolgreich waren. Der Landtag lehnte im Jahr 2002 einen Antrag der Fraktion Bündnis 90/Die Grünen („Stärkung der Demokratie und mehr Verwaltungstransparenz in Niedersachsen – Landtag macht sich stark für ein Informationsfreiheitsgesetz" – Drs. 17/2191) auf Schaffung eines IFG für Niedersachsen ab. Ein Antrag derselben Fraktion („Niedersachsen durch ein Informationsfreiheitsgesetz fit machen für die demokratische Wissensgesellschaft im 21. Jahrhundert" – Drs. 15/1027) aus der darauffolgenden Legislaturperiode hatte ebenfalls keinen Erfolg. 2009 schließlich fand auch der „Entwurf eines Gesetzes zur Regelung der Informationsfreiheit in Niedersachsen" (Drs. 16/1474) der Fraktion Bündnis 90/Die Grünen keine Zustimmung.

Der nächste Schritt: Verwaltung soll aktiv veröffentlichen

Parallel dazu gehen einige Bundesländer bereits einen Schritt weiter und gewähren den Zugang zu Verwaltungsinformationen nicht mehr nur auf Antrag sondern veröffentlichen die Informationen proaktiv. Nach § 11 Absatz 5 Bremer Informationsfreiheitsgesetz hat die Freie Hansestadt Bremen ein zentrales elektronisches Informationsregister eingerichtet, um das Auffinden der Informationen zu erleichtern und Informationen aus der Verwaltung kostenfrei zur Verfügung zu stellen. Hierzu gehören unter anderem alle bremischen Gesetze und Rechtsverordnungen, aber auch verwaltungsinterne Vorschriften und Beschlüsse. Das Hamburgische Transparenzgesetz (HmbTG) vom 6. Oktober 2012 führt zwei unterschiedliche Informationspflichten für die Verwaltung ein. Die eine Informationspflicht ist die Auskunftspflicht.



Nach § 2 Abs. 7 HmbTG bedeutet sie die Pflicht, Informationen auf Antrag und gegen Gebühr jedem zugänglich zu machen. Die andere ist nach § 2 Abs. 8 HmbTG die Pflicht, aktiv Informationen in ein Informationsregister einzustellen, das der Öffentlichkeit kostenfrei zur Verfügung stehen muss. Seit Sommer 2014 können nun unter anderem Bauleitpläne, Verträge zur Daseinsvorsorge, Gutachten oder Haushaltspläne der Staatsverwaltung von jedermann im „Transparenzportal Hamburg“ eingesehen werden. In Rheinland-Pfalz hat der Ministerrat Ende 2014 einen Gesetzesentwurf für ein Landes-Transparenzgesetz ins Beteiligungsverfahren übergeben, der in dieselbe Richtung geht. Bislang hatten die Bürger in Rheinland-Pfalz die Möglichkeit, ihren Anspruch auf Informationen durch einen Antrag geltend zu machen. Mit dem neuen Gesetz soll die Verwaltung zur aktiven Veröffentlichung verpflichtet werden. Nach den Plänen der Landesregierung soll das Gesetz nach der Sommerpause 2015 an den rheinland-pfälzischen Landtag gehen.

Somit entsteht in der Rechtsentwicklung der Bundesrepublik eine neue Generation von Informationszugangsgesetzen. Während die 1. Generation dieser Gesetze den Informationszugang auf Antrag gewährte, verpflichtet die 2. Generation nun öffentliche Stellen dazu, ihre Informationen proaktiv zu veröffentlichen und in eigens zu diesem Zweck konzipierte Transparenzregister einzustellen. Deutschland zeichnet damit eine Rechtsentwicklung nach, die im

europäischen Bereich schon weit fortgeschritten ist. Die Organe der Europäischen Union haben der Öffentlichkeit bereits weitgehende Zugangsrechte zu ihren Dokumenten eingeräumt. Das offene Datenportal der Europäischen Union bietet zentralen Zugang zu einem wachsenden Datenbestand der Institutionen und anderen Einrichtungen der EU. Die Daten können kostenlos zu gewerblichen und sonstigen Zwecken genutzt und weiterverwendet werden.

Der Grundsatz der Transparenz wurde 1991 durch den Vertrag von Maastricht eingeführt, um den demokratischen Charakter der Organe hervorzuheben. Der Rat und die Kommission haben in der Folge einen Verhaltenskodex für den Zugang zu ihren Dokumenten als zusätzlichen und wesentlichen Bestandteil ihrer Informations- und Kommunikationspolitik angenommen. 1996 wurde das Recht auf Informationszugang in Artikel 255 des Vertrags zur Gründung der Europäischen Gemeinschaft, heute Art. 15 des Vertrages über die Arbeitsweise der EU, verankert. Nach Verordnung (EG) Nr. 1049/2011 haben die Bürger das Recht auf Einsichtnahme in Dokumente des Europäischen Parlaments, des Rates und der Kommission. Bereichsspezifische Regelungen für die Mitgliedsstaaten existieren z. B. mit der Umweltinformationsrichtlinie aus dem Jahre 1990 (90/313/EG), die 2003 novelliert wurde (2003/4/EG). Aus demselben Jahr stammt auch die Richtlinie PSI (Public Sector Information, 2003/98/EG), geändert durch die neue PSI-Richtlinie 2013/37/EU. Sie enthält Regeln zur Weiterverwendung von Dokumenten, Daten und Informationen, die im Besitz öffentlicher Stellen der Mitgliedstaaten sind. Die Richtlinie PSI wird durch das Informationsweiterverwendungsgesetz (IWG) in Bundesrecht übertragen. Das IWG eröffnet zwar keine Zugangsrechte, normiert aber Mindeststandards für die Informationsverwertung öffentlicher Daten, die nach der jeweiligen Rechtslage frei zugänglich sind. Die Daten sollen in maschinenlesbarer Form, barriere- und diskriminierungsfrei bereitgestellt werden und sind zur Weiterverwendung zugelassen.

Mit der auf dem G8-Gipfel in Lough Erne im Juni 2013 beschlossenen Open-Data-Charta haben sich alle G8-Staaten zu einer breiten Veröffentlichung von Verwaltungsdaten im Sinne von Open Data bekannt. Die Bundesregierung hat sich in einem „nationalen Aktionsplan zur Umsetzung der Open Data Charter G8“ verpflichtet, entsprechende Maßnahmen für die weitere Öffnung von Verwaltungsdaten festzulegen. Dieser Aktionsplan wird sowohl auf der Bundesebene als auch gemeinsam mit den Ländern im IT-Planungsrat vorangetrieben. Einer der Grundsätze sieht dabei vor, Verwaltungsdaten grundsätzlich öffentlich zu machen und diese in einem Open-Data-Portal bereitzustellen.

Öffnung der Datenbestände nicht zulasten der Privatsphäre

Diesen aktuellen Entwicklungen darf sich Niedersachsen nicht verschließen. Sowohl ich selber, als auch meine Amtsvorgänger haben in unseren Tätigkeitsberichten und Stellungnahmen seit Ende der neunziger Jahre wiederholt gefordert, auch in Niedersachsen ein IFG zu erlassen. Diese Forderung erwächst nicht nur aus der Notwendigkeit einer Harmonisierung von Informationszugangsrechten in der EU und der Bundesrepublik oder der Notwendigkeit der Schaffung eines Rechtsrahmens zur Umsetzung des Aktionsplanes Open Government Data von Bund und Ländern. Aus meiner Perspektive ist es ebenso bedeutsam, im Blick zu behalten, dass Informationsfreiheit und Datenschutz zwei unverzichtbare Säulen der Informationsgesellschaft darstellen, die funktional eng miteinander verbunden sind (s. Kloepfer, Informationsfreiheit und Datenschutz: Zwei Säulen der Informationsgesellschaft,

DÖV, 2003, 221 und 225). Offenkundig ist aber auch, dass Informationsfreiheit und Datenschutz in einem Spannungsverhältnis stehen können. Dieses Spannungsverhältnis findet in der Befürchtung seinen Ausdruck, dass wichtige Rechtsgüter wie zum Beispiel die informationelle Selbstbestimmung, die öffentliche Sicherheit oder auch die Wahrung von Betriebs- und Geschäftsgeheimnissen durch die Informationsfreiheit verletzt werden könnten. Es ist ein besonderes Anliegen des Datenschutzes, dass die zunehmende Öffnung von Datenbeständen der öffentlichen Hand nicht zulasten des Schutzes der Privatsphäre geht. Unter Open Government Data dürfen daher keine personenbezogenen Daten fallen, sowie Informationen, deren Offenlegung eine Gefahr für die öffentliche Sicherheit bedeuten oder den Wettbewerb verzerren können.

Ich empfehle ausdrücklich die Schaffung eines konsistenten, datenschutzkonformen Rechtsrahmens für den Zugang zu Dokumenten, Informationen und den Datenbeständen der Verwaltung und zwar sowohl im Hinblick auf deren Zugänglichkeit als auch die Möglichkeiten ihrer weiteren Verwendung. Idealerweise sollten diese Regularien über die Grenzen bereichsspezifischer Normen hinweg harmonisiert werden. Ein Blick auf die Situation in den Bundesländern, die bereits eigene Informationsfreiheitsgesetze haben, zeigt, dass der vielbeschworene Zielkonflikt zwischen Transparenz und den datenschutzrechtlichen Belangen der Betroffenen durchaus praktikabel und sachgerecht zu lösen ist.

Es ist deshalb grundsätzlich sehr zu begrüßen, dass in Niedersachsen die Vorbereitungen für ein Informationsfreiheits- und Transparenzgesetz erneut angelaufen sind. SPD und Bündnis90/Die Grünen haben in Ihrer Koalitionsvereinbarung 2013–2018 vereinbart, „endlich auch in Niedersachsen eine umfassende Open-Data-Strategie mit einem modernen Informationsfreiheits- und Transparenzgesetz vorzulegen". In ihrer Sitzung vom 9. April 2013 hat die Landesregierung das Justizministerium beauftragt, den Gesetzesentwurf dazu federführend zu erarbeiten. Im Gesetzgebungsverfahren bin ich mit beratender Stimme beteiligt. In einem ersten Schritt wurde im Oktober 2013 vom Justizministerium ein ressortübergreifendes Fachgespräch auf Ebene der obersten Landesbehörden durchgeführt.

LfD mit beratender Stimme beteiligt

Der Schutz personenbezogener Daten muss weitgehend und präzise formuliert sein

Bereits im frühen Stadium der vorbereitenden Gespräche zum Gesetzesvorhaben wurde deutlich, dass die datenschutzrechtlich einwandfreie Behandlung sensibler, personenbezogener Daten ein wesentliches Regelungserfordernis der Norm werden wird. Dies umso mehr, als der Datenschutz in den bestehenden Gesetzen zur Informationsfreiheit grundsätzlich ein relativer Schutz ist. Das heißt, der Schutz personenbezogener Daten unterliegt im Regelfall einem Abwägungsvorbehalt. Ich werde mich im weiteren Fortgang des Gesetzgebungsverfahrens für einen möglichst weitgehenden und präzise formulierten Schutz personenbezogener Daten einsetzen. Ein dreistufiges Ausschlusskonzept hat sich hier bewährt. Der Informationszugang ist zu versagen, wenn er sich

- auf personenbezogene Daten bezieht,
- hierdurch schutzwürdige Interessen beeinträchtigt werden und
- keine überwiegenden Informationsinteressen vorliegen.

Von einer Interessenabwägung ausgenommen werden sollten besonders sensible Arten personenbezogener Daten sowie Informationen in Bezug auf Dienst-, Amts- und Mandatsverhältnisse. Dies betrifft insbesondere Informationen aus Personalakten (s. dazu Berger, Partsch, Roth, Scheel, IFG Kommentar, 2013).

Des Weiteren zeichnet sich in den ersten Gesprächen zu Struktur und Reglungsgehalt des Gesetzesentwurfs die Absicht ab, eine oder einen Landesbeauftragten für Informationsfreiheit einzurichten und diese Aufgabe der Landesbeauftragen für den Datenschutz zu übertragen. Diese Absicht befür-

worte ich ausdrücklich. Die Schaffung eines oder einer Landesbeauftragten für Informationsfreiheit hat sich in der Praxis mittlerweile durchgesetzt, zuletzt mit der Novellierung des Thüringer Informationsfreiheitsgesetzes. Das aus dem Jahre 2007 stammende Gesetz sah zunächst keinen Landesinformationsbeauftragten vor. Nach einer Evaluierung und der Novellierung mit dem Ziel der Stärkung der Informationsfreiheitsrechte und Schaffung eines Informationsfreiheitsbeauftragten ist das neue Gesetz seit dem 29. Dezember 2012 (Th. GVBl. 2012, 464) in Kraft. Damit sehen alle IFG der Länder und des Bundes die Einrichtung eines oder einer Informationsfreiheitsbeauftragten vor. Für die Rechtsstellung und organisatorische Anbindung der oder des Beauftragten für die Informationsfreiheit gibt es grundsätzlich verschiedene denkbare Konstellationen. In Kanada beispielsweise gibt es jeweils eine eigene Behörde für den Datenschutz und für die Informationsfreiheit. Beim Bund und den elf Bundesländern, die bereits über ein Landesinformationsfreiheitsgesetz verfügen, fand indes eine Bündelung der Aufgaben und Befugnisse zum Datenschutz und zur Informationsfreiheit statt, die sich bewährt hat. Die unabhängige Stellung der jeweiligen Beauftragten für den Datenschutz und deren hohe Fachkompetenz in Fragen der Wahrung von Privatsphäre und der Vertraulichkeit von Daten legen diese Zusammenführung nahe. Schließlich wird so auch einer Situation wirksam vorgebeugt, bei der zwei Beauftragte durch divergierende Stellungnahmen an die Öffentlichkeit treten.

Auch in den Behörden Ansprechpartner erforderlich

Darüber hinaus empfehle ich, die Einrichtung zentraler behördlicher Ansprechpartner für Informationsfreiheit im Landesgesetz zu verankern. In der Praxis hat sich eine zentrale Bearbeitung von Informationsfreiheitanträgen in den Behörden bewährt, sofern die Behördenstruktur diese Organisationsform prinzipiell zulässt. Von den im Rahmen der Evaluierung des Bundes-IFG befragten Behörden wurden in der Mehrzahl der Fälle Informationsfreiheitsbeauftragte eingerichtet (Drucksache 17/(4)522 B, S. 226 ff.). Die zu beobachtende Distanz zwischen den Informationszugang suchenden Bürgerinnen und Bürgern und den Behörden lässt sich durch die Einrichtung eines Informationsfreiheitsbeauftragten als behördlichen „Kümmerer" überbrücken. Für die Behörden bestünde ein Vorteil darin, dass ein solcher zentraler Ansprechpartner die Behördenleitung sowie die fachlich zuständigen Bearbeiter beratend unterstützt. Schließlich ermöglichte es die Einrichtung einer solchen Stelle, über alle Ebenen hinweg einen festen Erfahrungsaustausch zu institutionalisieren. Die bereits oben dargestellte sachliche Nähe zum Datenschutz legt nahe, die behördlichen Datenschutzbeauftragten mit der Aufgabe der behördlichen Informationsfreiheitsbeauftragten zu betrauen.
Im Lichte des stetig steigenden Anpassungsdrucks an europäische und bundesdeutsche Rechtsverhältnisse, des wachsenden Anspruchs der Bürgerinnen und Bürger an Transparenz, Beteiligung und Information sowie angesichts der Erfordernisse an einen datenschutzwahrenden Rechtsrahmen für eine Open-Government-Data-Strategie appelliere ich an die politischen Entscheidungsträger in Niedersachsen, nun den eingeschlagenen Weg fortzusetzen und die Umsetzung eines modernen Landesinformationsfreiheitsgesetzes zügig voranzubringen.

CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION
proklamiert in Nizza am 7. Dezember 2000 (2000/C 364/01)

Artikel 8
Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Niedersächsische Verfassung

Artikel 62
Landesbeauftragte oder Landesbeauftragter für den Datenschutz

(1) Die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz kontrolliert, dass die öffentliche Verwaltung bei dem Umgang mit personenbezogenen Daten Gesetz und Recht einhält. Sie oder er berichtet über ihre oder seine Tätigkeit und deren Ergebnisse dem Landtag.
(2) Der Landtag wählt auf Vorschlag der Landesregierung die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz mit einer Mehrheit von zwei Dritteln der anwesenden Mitglieder des Landtages, mindestens jedoch der Mehrheit seiner Mitglieder.
(3) Die Landesbeauftragte oder der Landesbeauftragte für den Datenschutz ist unabhängig und nur an Gesetz und Recht gebunden. Artikel 38 Abs. 1 und Artikel 56 Abs. 1 finden auf sie oder ihn keine Anwendung.
(4) Das Nähere bestimmt ein Gesetz. Dieses Gesetz kann personalrechtliche Entscheidungen, welche Bedienstete der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz betreffen, von deren oder dessen Mitwirkung abhängig machen. Der Landesbeauftragten oder dem Landesbeauftragten für den Datenschutz kann durch Gesetz die Aufgabe übertragen werden, die Durchführung des Datenschutzes bei der Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen zu kontrollieren.