daten
schutz

XXI. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2011 – 2012

XXI. Tätigkeitsbericht

der Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2011 – 2012

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

Zur besseren Lesbarkeit wird bei verallgemeinernden Substantiven lediglich das bestimmende grammatische Geschlecht verwendet. Selbstverständlich richtet sich dieser Bericht an die Angehörigen beider Geschlechter.

Inhaltsverzeichnis

Zu diesem Bericht

„Gut Ding will Weile haben“, sagt der Volksmund. Allerdings muss ich zugeben, dass sich der nun vorliegende Tätigkeitsbericht für die Jahre 2011 und 2012 außerordentlich viel „Weile“ gegönnt hat. Dennoch bin ich der festen Überzeugung, dass sich das Warten auf diesen Bericht gelohnt hat, denn er enthält erneut einen bunten Strauß an Themen, mit denen die unterschiedlichsten Facetten des Schutzes der Privatsphäre anschaulich beleuchtet werden.

Der Trend, der sich bereits im Tätigkeitsbericht für die Jahre 2009 und 2010 widerspiegelt, hat sich in den beiden darauf folgenden Jahren eindrucksvoll fortgesetzt: Der politische Kurswert des Datenschutzes hat erfreulicherweise weiter zugenommen und sowohl bei öffentlichen Stellen als auch im Bereich der Wirtschaft immer mehr an Bedeutung gewonnen – auch wenn es natürlich nach wie vor „schwarze Schafe“ gibt, die meinen, das Recht auf informationelle Selbstbestimmung anderweitigen Interessen unterordnen zu müssen.

Einen Schwerpunkt der Tätigkeit meiner Behörde haben im Berichtszeitraum die sozialen Netzwerke eingenommen. Der soziale Kontext, den z. B. Facebook schafft, um Daten über das Individuum, seine Interessen und sein Umfeld zu generieren, hat auch für Dritte unbestritten einen enormen Wert. Daraus resultiert wiederum der Wert dieser Internet-Unternehmen. Umso wichtiger ist es aus Sicht des Datenschutzes, hier Aufklärungsarbeit zu leisten und die vorhandenen Kontrollverluste und Rechtsverstöße nicht nur aufzuzeigen, sondern aus diesen Feststellungen die notwendigen Konsequenzen zu ziehen.

Ich wünsche Ihnen eine anregende Lektüre des Berichts und das eine oder andere „Aha-Erlebnis“.

Barbara Thiel
Landesbeauftragte für den Datenschutz

1 Datenschutz im öffentlichen Bereich

Live-Streams von Ratssitzungen: Besser nicht

Im Berichtszeitraum war bei den kommunalen Gebietskörperschaften zunehmend der Trend zur sogenannten Live-Stream-Übertragung von Rats- und Ausschusssitzungen ins Internet zu verzeichnen. Die kommunalpolitischen Akteure versprachen sich durch diese Technik eine breitere Öffentlichkeit. Als Vorbild dienten die Internetübertragungen der Sitzungen des Bundestages und der Länderparlamente.

Im Gegensatz zu den Abgeordneten des Bundestages und der Länderparlamente unterliegen die Abgeordneten der kommunalen Gebietskörperschaften als Teil der exekutiven Gewalt den datenschutzrechtlichen Bestimmungen des NDSG und anderer spezialgesetzlicher Regelungen. Dies hat zur Folge, dass die kommunalen Abgeordneten für die Datenübermittlung ins Internet eine Rechtsgrundlage benötigen. Die in Niedersachsen zur Datenübermittlung geltenden Bestimmungen reichen für einen Einsatz dieser Technik nicht aus. Deshalb ist die Übertragung einer öffentlichen Sitzung ins Internet nur dann rechtmäßig, wenn alle Beteiligten der Übertragung zugestimmt haben.

Auch rhetorische Fehlleistungen dauerhaft konserviert

In der Entscheidung des Bundesverwaltungsgerichts vom 3. August 1990 (7 C 14/90, NJW 1991, 118) zur Untersagung der Tonbandaufzeichnung durch einen Journalisten bei öffentlichen Gemeinderatssitzungen betonte das Gericht, dass eine „… von psychologischen Hemmnissen möglichst unbeeinträchtigte Atmosphäre zu den notwendigen Voraussetzungen eines geordneten Sitzungsbetriebs [gehört], den der Ratsvorsitzende zu gewährleisten hat. Das beruht auf dem legitimen, letztlich in der Gewährleistung der Selbstverwaltung durch Art. 28 Abs. 2 Satz 1 GG verankerten öffentlichen Interesse daran, dass die Willensbildung des Rates als demokratisch legitimierter Gemeindevertretung ungezwungen, freimütig und in aller Offenheit verläuft. Von daher kann die … Besorgnis nicht vernachlässigt werden, dass insbesondere in kleineren und ländlichen Gemeinden weniger redegewandte Ratsmitglieder durch das Bewusstsein des Tonmitschnitts ihre Spontaneität verlieren, ihre Meinung nicht mehr ‚geradeheraus' vertreten oder schweigen, wo sie sonst gesprochen hätten. Denn Tonbandaufzeichnungen zeitigen nun einmal für das Verhalten der Betroffenen

erhebliche Wirkung, weil sie jede Nuance der Rede, einschließlich der rhetorischen Fehlleistungen, der sprachlichen Unzulänglichkeiten und der Gemütsbewegungen des Redners, dauerhaft und ständig reproduzierbar konservieren.“ Diese Grundsätze gelten erst recht bei Ton- und Bildaufnahmen, wie es bei einer Übertragung im Internet der Fall ist.
Auch wenn zwischenzeitlich Entscheidungen (z. B. VG Saarland, Az: 3 K 501/10) die Zulassung von Filmaufnahmen bei öffentlichen Stadtratssitzungen zu Sendezwecken durch einen (privaten) regionalen Rundfunkveranstalter für zulässig halten, besteht jedoch keine Rechtsgrundlage für die Übertragung ins Internet. Zu bedenken ist bei diesem Verfahren auch, dass die kommunale Gebietskörperschaft die Herrschaft über ihre Daten aufgibt. Denn bei einer Übertragung der Daten ins Internet ist nicht absehbar, wer, wann, wo und zu welchem Zweck die Daten verarbeitet und in welcher Art und Weise sie weiterverwendet werden.

Nur mit Einwilligung

Entscheiden sich die politischen Akteure dennoch für einen Einsatz dieser Technik, ist stets darauf zu achten, dass nur die Abgeordneten zu sehen und zu hören sind, die ihre Einwilligung erklärt haben. Zudem muss immer gewährleistet sein, dass sämtliche Wortmeldungen von Bürgerinnen und Bürgern, die keine Abgeordneten sind, von der Übertragung ausgeschlossen sind. Das gilt grundsätzlich auch für Zwischenrufe. Die erteilte Einwilligungserklärung kann jederzeit, auch während der gerade stattfindenden Sitzung, mit Wirkung für die Zukunft widerrufen werden.
Ich empfehle daher den kommunalen Gebietskörperschaften – auch aufgrund ihres örtlich begrenzten Wirkungskreises – von der Live-Stream-Übertragung von Rats- und Ausschusssitzungen Abstand zu nehmen.

Weitere Informationen:

www.lfd.niedersachsen.de
>Themen >Kommunales >Orientierungshilfe zum Datenschutz für kommunale Abgeordnete

Personalaktendaten:
Endlich wieder Regelungsgleichklang für alle Beschäftigten im öffentlichen Dienst

Um unterschiedliche Standards beim Schutz von Personaldaten zu vermeiden, forderte ich in den vergangenen Jahren, dass die für Beamtinnen und Beamte bestehenden spezialgesetzlichen Regelungen zum Personaldatenschutz auch für das Tarifpersonal und sonstige Beschäftigte im Land Niedersachsen gelten sollen. Zu begrüßen ist daher die seit Dezember 2012 geltende Änderung des § 24 Abs. 1 Niedersächsisches Datenschutzgesetz (NDSG):

„Die beamtenrechtlichen Vorschriften über die Führung von Personalakten gemäß § 50 des Beamtenstatusgesetzes und §§ 88 bis 95 des Niedersächsischen Beamtengesetzes sind für alle nicht beamteten Beschäftigten einer öffentlichen Stelle entsprechend anzuwenden, soweit tarifvertraglich nichts anderes geregelt ist.“

Die aktuelle Regelung stellt den Gleichklang der Vorgaben sowohl für Personaldaten (§ 88 Abs. 1 NBG) als auch für besonders sensibel zu handhabende Personalaktendaten (§ 50 BeamtStG, §§ 88 Abs. 2 bis 95 NBG) her. Unterstrichen wird diese Absicht des Gesetzgebers durch die Begründung zu § 24 NDSG, wonach die Vorschriften zur Personaldatenverarbeitung der beamteten und nicht beamteten Beschäftigten des öffentlichen Dienstes wieder einander angeglichen werden sollen (siehe Begründung B, zu Nr. 2 – § 24 n. F. der Landtags-Drucksache 16/5182).

Weitere Informationen:

www.lfd.niedersachsen.de
>Recht >Nieders. Recht

Datenweitergabe an Privatärztliche Verrechnungsstellen: Einwilligungserklärung soll verbessert werden

Aus Zeit- und Kostengründen rechnen viele Ärzte die erbrachten Leistungen nicht mehr selbst mit den Privatpatienten ab, sondern überlassen die Rechnungserstellung und Forderungseinziehung einer Privatärztlichen Verrechnungsstelle (PVS). Dies sind in der Regel ärztlich geleitete berufsständische Einrichtungen, welche sich auf die Rechnungserstellung und Forderungseinziehung spezialisiert haben. Damit Ärzte die für die Erstellung der Rechnung erforderlichen Daten an eine PVS übermitteln dürfen, ist eine Einwilligungserklärung erforderlich. Diese Vordrucke erhalten die Ärzte von der jeweiligen PVS.

Immer wieder erreichen mich Eingaben von Patienten, welche die Abrechnung der ärztlichen Leistungen von einer PVS erhalten und angeben, keine Einwilligung erteilt zu haben. Die Ärzte, die mit der PVS Niedersachsen zusammenarbeiten, verpflichten sich gegenüber der PVS dazu, Daten nur mit Einwilligung der Patienten zu übermitteln. Die PVS Niedersachsen speichert die patientenbezogenen Daten nur solange, wie sie für das Abrechnungsverfahren benötigt werden. Sie darf sich daher darauf verlassen, dass dem Arzt die Einwilligung vorliegt. Verlangte man, dass die Ärzte bei jeder Abrechnung eine aktuelle Einwilligungserklärung einholen sollen, bedeutete dies einen Mehraufwand für alle Beteiligten, der gerade bei den Patienten nicht auf Akzeptanz stieße. Verantwortlich für die Einholung der Einwilligung sind die Ärzte. Diese dürfen nur von denjenigen Patienten Daten an die PVS übermitteln, von denen eine Einwilligungserklärung vorliegt. Sie wird derzeit beim ersten Arztbesuch unterzeichnet und verbleibt beim Arzt. Auf Nachfrage bei den behandelnden Ärzten stelle ich häufig fest, dass die Patienten doch eine entsprechende Einwilligungserklärung unterzeichnet, dies jedoch vergessen haben.
Ich befinde mich aktuell in konstruktiven Gesprächen mit einer privatärztlichen Verrechnungsstelle, die sich mit der Bitte um Beratung an mich gewandt hatte. Ziel ist es, die vorhandene Einwilligungserklärung zu überarbeiten und den bereits hohen datenschutzrechtlichen Anforderungen genügenden Verfahrensablauf noch weiter zu verbessern, ohne einen bürokratischen Aufwand für die Patienten und alle anderen Beteiligten zu verursachen, der in keinem angemessenen Verhältnis stünde.

Das neue Patientenrechtegesetz: Information über Behandlungsfehler nur auf Nachfrage

Im Januar 2012 wurde der Öffentlichkeit ein Gesetzentwurf zur Verbesserung der Rechte von Patientinnen und Patienten vorgestellt. In diesem Patientenrechtegesetz sollten insbesondere die bislang von den Gerichten entwickelten Grundsätze des Arzthaftungs- und Behandlungsrechts zusammengeführt und transparent für alle an einer Behandlung Beteiligten geregelt werden. Das Patientenrechtegesetz findet sich in den §§ 630a bis 630h des Bürgerlichen Gesetzbuches (BGB). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßte den Gesetzesentwurf grundsätzlich, forderte aber mit einer Entschließung vom 23.5.2012 die Bundesregierung nachdrücklich auf, den Gesetzesentwurf zu überarbeiten und weitere wichtige datenschutzrechtliche Aspekte mit aufzunehmen.

Die Datenschutzbeauftragten forderten im Einzelnen:

- Die vertraglichen Offenbarungsobliegenheiten der Patientinnen und Patienten gegenüber den Behandelnden dürfen nicht ausgeweitet werden. Die Patientinnen und Patienten dürfen nicht zur Offenlegung von Angaben über ihre körperliche Verfassung verpflichtet werden, die keinen Behandlungsbezug haben.
- Die Patientinnen und Patienten müssen in jedem Fall und nicht erst auf Nachfrage über erlittene Behandlungsfehler informiert werden.
- Der Gesetzentwurf sollte im Zusammenhang mit der Behandlungsdokumentation um verlässliche Vorgaben zur Absicherung des Auskunftsrechts der Patientinnen und Patienten sowie zur Archivierung und Löschung ergänzt werden.
- Der Zugang der Patientinnen und Patienten zu der sie betreffenden Behandlungsdokumentation darf nur in besonderen Ausnahmefällen eingeschränkt werden. Die in dem Entwurf vorgesehenen Beschränkungen sind zu weitgehend und unpräzise. Zudem sollte klargestellt werden, dass auch berechtigte eigene Interessen der Angehörigen einen Auskunftsanspruch begründen können.
- Der Gesetzentwurf ist um Regelungen zur Einbeziehung Dritter im Rahmen eines Behandlungsvertrages (Auftragsdatenverarbeitung) zu ergänzen.
- Regelungsbedürftig ist ferner der Umgang mit der Behandlungsdokumentation beispielsweise im Falle eines vorübergehenden Ausfalls, des Todes oder der Insolvenz des Behandelnden. Im Bereich der Heilberufe fehlt es – anders als zum Beispiel bei den Rechtsanwälten – an einem bundesweit einheitlichen Rechtsrahmen.

Leider wurde der Großteil dieser Anregungen nicht in das am 26.2.2013 in Kraft getretene Patientenrechtegesetz aufgenommen. Als eine der positiven Ausnahmen ist die Klarstellung in § 630g BGB zu nennen, dass nunmehr auch für Patientendaten ein umfassendes Einsichtsrecht für die Betroffenen besteht. Eine Beschränkung auf objektive Befunde, wie sie noch § 10 der Berufsordnung der Ärztekammer Niedersachsen vorsieht, kommt daher nicht mehr in Betracht. In § 630g BGB ist eine Einschränkung des Einsichtsrechts nur dann vorgesehen, wenn erhebliche therapeutische Gründe oder Rechte Dritte entgegen stehen. Eine solche Ablehnung ist zu begründen. Diese Regelung ist nachvollziehbar.

Entschließungen der Konferenz der Datenschutz-beauftragten:
www.lfd.niedersachsen.de >Allgemein >DSB-Konferenzen >Entschließungen

Datenschutz im Krankenhaus: Neue Orientierungshilfe schützt vor Pannen

Gesundheitsdaten gehören zu den sensibelsten Daten eines Menschen. In den Datenschutzgesetzen und der Vorschrift zur ärztlichen Schweigepflicht des § 203 Strafgesetzbuch (StGB) steht, dass Dritte ohne besondere Befugnis Gesundheitsdaten weder einsehen noch weitergeben dürfen. Bereits der Eid des Hippokrates (um 460 bis 370 v. Chr.) enthält die Selbstverpflichtung: „Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als ein Geheimnis betrachten." Man sollte daher davon ausgehen, dass in Krankenhäusern für diese Daten ein besonders hoher Schutz gewährleistet ist. Dies trifft allerdings nicht immer zu.

Stellen Sie sich vor, Sie haben einen schweren Unfall und kommen in ein Krankenhaus, in welchem Sie aufgrund von Komplikationen mehrere Monate verbringen. Wer könnte sich für Ihre Gesundheitsdaten interessieren? Verwandte, Freunde, Bekannte, Kollegen? In der Regel wollen Sie sicherlich selbst entscheiden, wem Sie welche Daten anvertrauen. Durch die fortschreitende Technik in den Krankenhäusern hat die alte Papierakte am Krankenbett ausgedient, und alle Daten eines Patienten werden in dem aus vielen verschiedenen Komponenten bestehenden Krankenhausinformationssystem (KIS) gespeichert. Für die behandelnden Ärztinnen und Ärzte ist dies ein sehr guter Fortschritt, sie erkennen auf einen Blick alle wichtigen Daten des Patienten, wodurch die Behandlung sicherlich verbessert werden kann. Sofern nur die an der Behandlung des Patienten beteiligten Personen die Daten einsehen können, sind diese Systeme zu begrüßen.

Doch genau an diesem Punkt hakt es bei vielen Krankenhäusern. In einigen Fällen konnte sogar jede im Krankenhaus beschäftigte Person die Daten aller Patientinnen und Patienten einsehen. Handelt es sich bei dem Patienten um einen unscheinbaren Bürger, ist die Neugierde sicherlich nicht hoch, wissen zu wollen, an welchen Erkrankungen dieser leidet. Anders ist es anscheinend, wenn es sich um eine durch Fernsehen, Sport oder Politik recht populäre Person handelt. Kenntnis davon erhielten die Datenschutzaufsichtsbehörden durch einen Vorfall aus dem Jahre 2009, als in der Presse Details zu dem Gesundheitszustand einer Fernsehmoderatorin zu lesen waren, die nicht für die Öffentlichkeit bestimmt und von der betroffenen Person auch nicht an die Presse gegeben worden waren. Im darauf folgenden Ermittlungsverfahren kam heraus, dass nicht nur eine Person unberechtigterweise auf die im KIS gespeicherten Daten zugegriffen hatte, sondern eine Vielzahl von an der Behandlung nicht beteiligten Beschäftigten.

In einigen Fällen konnte sogar jede im Krankenhaus beschäftigte Person die Daten aller Patientinnen und Patienten einsehen

Orientierungshilfe soll Abhilfe schaffen

Der Hamburgische Datenschutzbeauftragte hat diesen Vorfall zum Anlass genommen, ein Eckpunktepapier zu erarbeiten, das den Krankenhäusern helfen soll, den Datenschutz besser zu wahren. Auf der Grundlage dieses Eckpunktepapiers wurde unter der Federführung des Berliner Beauftragten für Datenschutz und Informationsfreiheit von einer Unterarbeitsgruppe der Arbeitskreise „Gesundheit und Soziales" und „Technik" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter meiner Beteiligung die Orientierungshilfe Kran-

kenhausinformationssysteme (OH-KIS) erarbeitet. Neben Vertretern der Landesdatenschutzbeauftragten haben auch Datenschutzbeauftragte der beiden großen Kirchen in Deutschland teilgenommen. Adressaten der OH-KIS sind die Krankenhäuser (unabhängig von der Trägerschaft) und die Hersteller von Krankenhausinformationssystemen.
Die OH-KIS besteht aus zwei Teilen. Der erste Teil stellt die Rechtsfolgen der datenschutzrechtlichen Regelungen und die Vorgaben zur ärztlichen Schweigepflicht dar, wie sie von den Datenschutzbeauftragten ausgelegt werden. Anhand von Szenarien im Krankenhaus wird beschrieben, was aus datenschutzrechtlicher Sicht jeweils zu beachten ist. Hier werden bereits klare Aussagen getroffen, welche Mitarbeiter eines Krankenhauses wann Zugriff auf welche Daten haben dürfen. Der im Datenschutz allgegenwärtige Grundsatz der Erforderlichkeit gilt auch für die Beschäftigten und Ärzte im Krankenhaus. Ziel ist es, dass das Krankenhaus sicherstellt, dass nur diejenigen Personen auf die Patientendaten zugreifen, welche diese im aktuellen Behandlungs- oder Pflegefall tatsächlich benötigen. Gleichzeitig muss sichergestellt werden, dass einem Arzt im Falle eines Notfalls ohne großen Zeitverlust schnellstmöglich alle notwendigen Daten des Patienten zur Verfügung stehen, unabhängig davon, ob dieser schon einmal von ihm behandelt wurde oder nicht.
Im zweiten Teil der OH-KIS werden sowohl den Betreibern, als auch den Herstellern mögliche Maßnahmen vorgeschlagen, wie eine datenschutzgerechte technische Umsetzung erfolgen kann.

Einigkeit in Niedersachsen

Wir haben bereits frühzeitig Gespräche mit der Niedersächsischen Krankenhausgesellschaft zum ersten Teil der OH-KIS geführt. In fast allen Punkten bestand Einigkeit bei der Rechtsauslegung, unter Berücksichtigung der Tatsache, dass ein vollumfänglich datenschutzgerechter Betrieb eines Krankenhauses aufgrund der Vielzahl der eingesetzten Systeme nicht von heute auf morgen möglich ist. Zum zweiten Teil wird die Deutsche Krankenhausgesellschaft noch eine Art Leitfaden herausgeben. Unabhängig hiervon bleiben wir in Gesprächen mit der Niedersächsischen Krankenhausgesellschaft sowie mit den Datenschutzbeauftragten verschiedener Krankenhäuser in Niedersachsen.

Orientierungshilfe zeigt Wirkung

Die Herausgabe der Orientierungshilfe KIS hat bereits zu einer gestiegenen Wertigkeit des Datenschutzes in Krankenhäusern geführt. Die ersten Schritte in die richtige Richtung sind getan. Auch wenn die technische Entwicklung viel Zeit benötigt, so kann doch jede Mitarbeiterin und jeder Mitarbeiter eines Krankenhauses durch das eigene Verhalten (nicht aus reiner Neugierde in fremde Daten schauen, die bekannten Informationen nicht an unbefugte Dritte weitergeben) für den Datenschutz viel mehr erreichen, als es Kontrollen oder Sanktionen könnten.

Weitere Informationen:

www.lfd.niedersachsen.de
>Themen >Gesundheit >Krankenhaus

Antragsvordrucke: Behörden oft zu neugierig

Die Prüfung von Antragsvordrucken auf deren datenschutzrechtliche Zulässigkeit gehört sicherlich nicht zu den publikumswirksamsten Tätigkeiten eines Datenschützers. Sie ist jedoch unabdingbar, weil die Vordrucke als Instrument für die Erhebung von oft hochsensiblen persönlichen Daten und damit der Erfassung der Persönlichkeit dienen. In der Regel werden die Antragsvordrucke von den verantwortlichen Stellen in Zusammenarbeit mit den entsprechenden Fachabteilungen entworfen. An die Beteilung der behördlichen Datenschutzbeauftragten vor Ort wird jedoch leider eher selten gedacht.

Antragsvordrucke sind auch in der heutigen Zeit noch das Mittel der Datenerhebung. Eine Behörde darf jedoch nur die Daten erheben, welche für die gesetzliche Aufgabenerfüllung erforderlich sind. Aus Gründen der Arbeitserleichterung gibt es Daten, die eine Behörde gerne erheben würde, diese jedoch nicht zwingend für die Aufgabenerledigung benötigt. Diese sogenannten „Nice-to-have-Daten" dürfen mangels einer gesetzlichen Grundlage grundsätzlich nicht erhoben werden. Allenfalls die Erhebung von Daten, die zwar nicht zwingend erforderlich sind, jedoch die Kommunikation mit den Betroffenen erleichtern können, wie zum Beispiel Telefonnummer oder E-Mail-Adresse, erachte ich für zulässig, wenn diese als „Freiwillige Angabe" gekennzeichnet sind und nur für diesen Zweck genutzt werden. Werden in den Antragsvordrucken wirklich nur die erforderlichen Daten abgefragt, ist dies bereits ein wichtiger Schritt zur datenschutzgerechten Aktenführung.
In den letzten Jahren habe ich Antragsvordrucke verschiedener Stellen überprüft und Änderungsverfahren begleitet. In der Regel umfassen bereits einfache Exemplare mehrere Seiten. Die Prüfung nimmt nicht selten mehrere Tage in Anspruch. Gerade im Sozialbereich müssen oft mehrere Gesetze und entsprechende Kommentarliteratur zu Rate gezogen werden. Nach einem ersten Überblick folgen oft mehrere Gespräche mit der verantwortlichen Stelle, deren Fachbereichen und behördlichen Datenschutzbeauftragten, um jede einzelne Frage des Vordrucks auf deren Erforderlichkeit zu überprüfen. In den meisten Fällen wurden die Vordrucke bereits zeitnah angepasst, sodass eine datenschutzgerechte Datenerhebung nunmehr gewährleistet ist.
Im Folgenden sind einige Beispiele für eine solche Überprüfung aufgeführt:

Einführung des Bildungs- und Teilhabepaketes

Seit der Einführung des so genannten Bildungs- und Teilhabepaketes zum 1. April 2011 können Kindern und Jugendlichen aus einkommensschwachen Familien zusätzliche Leistungen zur Verbesserung der Teilhabemöglichkeiten an schulischer und außerschulischer Bildung sowie an kulturellen Angeboten in Anspruch nehmen. Nach Einschätzung des Bundesministeriums für Arbeit und Soziales sind bun-

desweit über 2,5 Millionen Kinder und Jugendliche anspruchsberechtigt, da sie Leistungen der Grundsicherung für Arbeitssuchende (SGB II), der Sozialhilfe (SGB XII), Wohngeld, Kinderzuschlag oder Leistungen nach dem Asylbewerberleistungsgesetz (AsylbLG) beziehen. Welche Leistungen das Bildungs- und Teilhabepaket umfasst, ist bundeseinheitlich in den o. g. Gesetzen geregelt.
Leider wurde es versäumt, den zuständigen Stellen ein datenschutzrechtlich geprüftes Antragsmuster zur Verfügung zu stellen, an dem sich die einzelnen Leistungsträger im Rahmen ihrer kommunalen Unabhängigkeit hätten orientieren können. Dies führte dazu, dass jede Kommune ihren eigenen Antragsvordruck für die Leistungen des Bildungs- und Teilhabepaketes entwickelt und hierbei teilweise mehr als die erforderlichen Daten von den Leistungsempfängern abgefragt hat. Nachdem ich durch verschiedene Eingaben hierauf aufmerksam geworden war, habe ich die verantwortlichen Stellen gebeten, ihre Vordrucke datenschutzgerecht zu gestalten. Meine Änderungsvorschläge wurden in allen Fällen umgesetzt, sodass erfreulicherweise die Anzahl der Eingaben in diesem Bereich mittlerweile stark zurückgegangen ist.

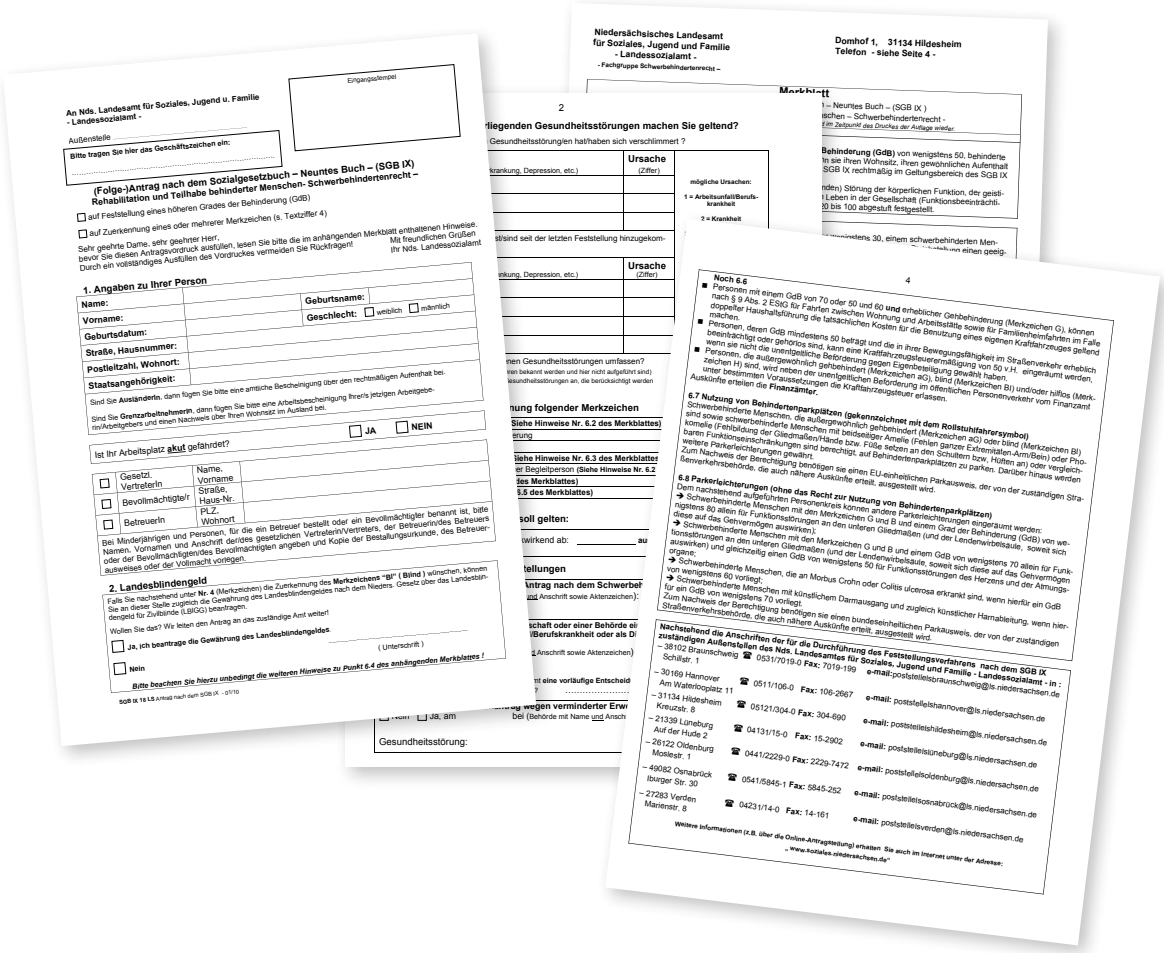
Anträge auf Rehabilitation und Teilhabe behinderter Menschen beim Landessozialamt

Im Rahmen der Feststellungsverfahren nach dem Sozialgesetzbuch – Neuntes Buch (SGB IX) – müssen immer hochsensible Gesundheitsdaten erhoben und verarbeitet werden. Muss das Landesamt für Soziales, Jugend und Familie (Landessozialamt) medizinische Daten bei behandelnden Ärzten des Antragstellers erheben, wird eine Entbindung von der ärztlichen Schweigepflicht benötigt. Die bisher verwendete Erklärung war sehr pauschal gehalten. Hierüber haben sich sowohl Ärzte, als auch Antragsteller bei mir beschwert. Genau wie eine Einwilligungserklärung im Datenschutzrecht muss auch eine Entbindung von der ärztlichen Schweigepflicht möglichst präzise auf den aktuellen Fall zugeschnitten sein, damit sie wirksam ist. Gleichzeitig muss jedoch auch der Arbeitsaufwand betrachtet werden, der entstünde, wenn das Landessozialamt für jeden Antragsteller eine individuelle Entbindungserklärung anfertigte. Die Schwierigkeit bei solchen Erklärungen liegt immer darin, möglichst präzise den aktuellen Sachverhalt zu erfassen, den Antragsteller über den Sinn und Zweck der Datenerhebung zu informieren und ihn auf die Freiwilligkeit und Widerrufsmöglichkeiten, aber auch auf seine gesetzlichen Mitwirkungspflichten hinzuweisen. Gleichzeitig soll die Erklärung so verständlich wie möglich formuliert sein, als Vordruck für viele Antragsteller eingesetzt werden können und möglichst den Umfang von einer Seite nicht überschreiten.
Dank der sehr guten Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten des Landessozialamtes in Hildesheim konnte ein Vordruck erarbeitet werden, der die genannten Voraussetzungen erfüllt.

Ärztliche Bescheinigung – Mehrbedarf wegen kostenaufwändiger Ernährung

Leiden Sozialleistungsbezieher an bestimmten Krankheiten, kann es erforderlich sein, dass sie auf eine bestimmte Ernährung angewiesen sind. Eine solche Ernährung verursacht Kosten, die mit den allgemeinen Regelsätzen für Leistungsempfänger nicht gedeckt werden können. In diesen Fällen erhalten die Betroffenen einen erhöhten Leistungsbetrag. Die zahlende Stelle muss natürlich die Möglichkeit haben, zu überprüfen, ob ein Mehrbedarf aufgrund einer Erkrankung gerechtfertigt ist. Hierzu müssen verschiedene medizinische Daten erhoben werden.

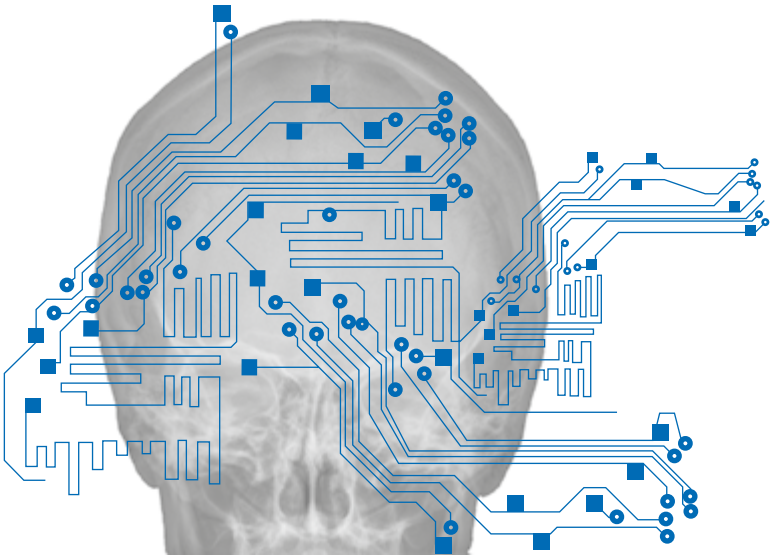
Eine Bürgerin hat sich bei mir erkundigt, ob es in jedem Falle erforderlich sei, dass der medizinische Dienst die Angaben zur Größe, Gewicht und dem sich hieraus ergebenen Body-Mass-Index (BMI) erhalten solle. Diese würden mit dem Standardvordruck immer abgefragt. Tatsächlich ist es so, dass diese Angaben nur bei bestimmten Erkrankungen erforderlich sind. Lediglich wenn der BMI unter 18,5 liegt und das Untergewicht die Folge einer Erkrankung ist, bedarf es hierzu einer Aussage des Arztes, in allen anderen Fällen jedoch nicht. Ich habe der verantwortlichen Stelle mitgeteilt, dass der Vordruck entsprechend angepasst werden muss. Dies wurde zeitnah umgesetzt und auf dem Vordruck klargestellt, dass diese Angaben nur in Ausnahmefällen erforderlich sind.



Früherkennungsuntersuchungen von Kindern: Landessozialamt darf Jugendämter informieren

In der Vergangenheit haben Medien immer wieder über Fälle von Verwahrlosung und Kindeswohlgefährdung berichtet. Beispiele sind der zwei Jahre alte Kevin aus Hamburg oder die fünf Jahre alte Lea-Sophie aus Schwerin. Um das Wohl der Kinder besser zu schützen, wurde, wie in vielen anderen Bundesländern, auch in Niedersachsen ein Gesetz erlassen, das den öffentlichen Stellen die Möglichkeit eröffnet, derartige Fälle frühzeitig zu erkennen und hoffentlich zu verhindern.

Am 28.10.2009 wurde das Niedersächsische Gesetz über das Einladungs- und Meldewesen für Früherkennungsuntersuchungen von Kindern (NFrüherkUG) verkündet. In das Gesetzgebungsverfahren war ich bereits frühzeitig eingebunden, und meine datenschutzrechtlichen Anregungen wurden größtenteils angenommen. Seit dem 1.4.2010 erhalten die gesetzlichen Vertreter aller in Niedersachsen lebenden Kinder vom Niedersächsischen Landesamt für Soziales, Jugend und Familie (Landessozialamt) ein Einladungsschreiben zu der jeweiligen sogenannten U-Untersuchung, die für das jeweilige Lebensalter des Kindes vorgesehen ist (U1 bis U9). Dem Einladungsschreiben beigefügt ist eine Rückmeldekarte, auf welcher der untersuchende Arzt bestätigt, dass das Kind an der U-Untersuchung teilgenommen hat. Inhalte der Untersuchung oder Diagnosen werden nicht mitgeteilt.
Liegt dem Landessozialamt innerhalb einer gewissen Frist keine Rückmeldung vor, erhalten die gesetzlichen Vertreter eine Erinnerung, die U-Untersuchung ihres Kindes wahrzunehmen. Sollte auch nach diesem Erinnerungsschreiben keine Rückmeldung beim Landessozialamt eingehen, muss gemäß § 4 Abs. 2 NFrüherkUG das zuständige Jugendamt informiert werden. Dort wird das weitere Vorgehen geprüft. In der Regel wird den Eltern angeboten, im Rahmen eines Hausbesuchs den Sinn und Zweck der U-Untersuchungen noch einmal darzulegen. Die Nicht-Rücksendung der Bestätigung der Teilnahme an der U-Untersuchung allein ist jedoch aus Sicht der Arbeitsgemeinschaft der Jugendämter der Länder Niedersachsen und Bremen noch kein Grund für den Verdacht einer Kindeswohlgefährdung.
Bei Beschwerden der gesetzlichen Vertreter gegen dieses Verfahren weise ich darauf hin, dass für die Datenübermittlung eine klare gesetzliche Grundlage besteht, gegen die aus datenschutzrechtlicher Sicht keine Einwände zu erheben sind.



Verarbeitung von Gesundheitsdaten: Zahl neuer Projekte stark angestiegen

In den vergangenen zwei Jahren wurden viele neue Verfahren zur Datenverarbeitung im Gesundheitswesen entwickelt. So ist es nicht überraschend, dass die Anzahl der mir bereits vor Veröffentlichung vorgestellten Projekte im Vergleich zum vorherigen Berichtszeitraum auf zehn angestiegen ist und sich damit mehr als verdoppelt hat.

Einige dieser Projekte sollen den Datenaustausch zwischen behandelnden Ärzten durch Schaffung von Gesundheitsnetzen beschleunigen und dem Patienten Arbeit abnehmen, andere die konsiliarische Beratung der behandelnden Ärzte verbessern. Wieder andere möchten die gespeicherten Patientendaten in die „Cloud" auslagern. Die meisten Projekte sollen eine bessere und schnellere Behandlung der Patientinnen und Patienten erlauben und zudem Kosten sparen. In der akuten Krankheitssituation werden sich die wenigsten Menschen Gedanken über den Verlauf ihrer Daten machen. Wenn die Daten von Dritten missbraucht werden sollten, kann dies jedoch weitreichende Folgen haben. Gesundheitsdaten sind die sensibelsten Daten eines Menschen, mit denen sehr viel Unheil angerichtet werden kann, so sie in unbefugte Hände gelangen.
Aus diesem Grund habe ich wünschenswerte und positive Entwicklungen in der Technik des Gesundheitswesens aufmerksam zu betrachten. Ich vertrete die Auffassung, dass Datenschutz nicht „verhindern", sondern vor negativen Folgen bewahren soll. Als Datenschutzbeauftragter bin ich verpflichtet, darauf zu achten, dass diese Projekte auch aus datenschutzrechtlicher Sicht zulässig sind. Aufgefallen ist mir, dass sich das Datenschutzbewusstsein in den letzten Jahren auch auf Seiten der Hersteller neuer Programme positiv entwickelt hat. Bei einigen Projekten bestand datenschutzrechtlicher Nachholbedarf. Hier wurden meine Anregungen aufgenommen, und sie sollen in das endgültige Produkt integriert werden.

Nach ELENA-Stopp: OMS und Bea sollen es besser machen

Im Juli 2011 wurde das ELENA-Verfahren (Elektronisches Entgeltnachweisverfahren), das jahrelang für Gesprächstoff gesorgt hatte, überraschend von der Bundesregierung eingestellt. Schon in meinen vorangegangenen Tätigkeitsberichten (XX. Tätigkeitsbericht, S. 14, und XIX. Tätigkeitsbericht, S. 14) habe ich über ELENA informiert. Zwei Nachfolgeverfahren sollen es jetzt besser machen.

ELENA verfolgte nach Ansicht der Bundesregierung zwei Ziele: Bürokratieabbau und Einsatz von innovativer Technik. Die Bürger sollten im Falle der Beantragung von Sozialleistungen von einer beschleunigten und diskreten Abwicklung profitieren. Sozialleistungsträger, etwa die Agentur für Arbeit bei der Berechnung von Arbeitslosengeld, sollten bei Bedarf entsprechende Daten bei der so genannten Zentralen Speicherstelle abrufen können. Die Ausstellung einer Entgeltbescheinigung durch den Arbeitgeber wäre dann nicht mehr erforderlich gewesen. Hierzu sollten die Arbeitgeber eine qualifizierte Signatur verwenden. Die Kritiker des ELENA-Verfahrens sahen in dem Ausmaß der Datenspeicherung (Daten von 35 bis 40 Millionen abhängig Beschäftigten), die auch Personengruppen wie zum Beispiel Beamte beinhaltete, die nicht verwandt worden wären, eine Vorratsdatenspeicherung. Die Einstellung des ELENA-Verfahrens ist offiziell von der Bundesregierung mit der fehlenden Verbreitung der elektronischen Signatur bei den Arbeitgebern und mit dem auch „in absehbarer Zeit nicht flächendeckend“ zu erreichenden notwendigen datenschutzrechtlichen Sicherheitsstandard begründet worden.
Die Nachfolgeverfahren OMS (Optimiertes Meldeverfahren in der sozialen Sicherung) und das Projekt Bea (Bescheinigung elektronisch annehmen) werden im folgenden vorgestellt:

OMS noch in der Optimierungsphase

Eine Vorratsdatenspeicherung, wie sie ELENA von Kritikern vorgeworfen wurde, muss ausgeschlossen sein.

Das Projekt OMS startete am 15.2.2012 und umfasst alle Bereiche der Sozialversicherung. Durchgeführt wird in dem Projekt eine zweijährige Untersuchung der bestehenden elektronischen Arbeitgebermeldeverfahren in der sozialen Sicherung mit dem Ziel, sie zu optimieren und zu vereinfachen. Das Projekt, das auf einen Beschluss des Bundeskabinetts vom 21. September 2011 zurückgeht, wird von der Informationstechnischen Servicestelle der gesetzlichen Krankenversicherung GmbH (ITSG GmbH) umgesetzt und vom Bundesbeauftragten für Datenschutz und die Informationsfreiheit datenschutzrechtlich begleitet. Die erste Projektphase der Status-quo-Erhebung der betrachteten Meldeverfahren ist am 31.8.2012 abgeschlossen worden. Danach handelt es sich um insgesamt zehn Meldeverfahren, zwölf Be-

oms

OPTIMIERTES MELDEVERFAHREN
IN DER SOZIALEN SICHERUNG

WWW.PROJEKT-OMS.DE

scheinigungsverfahren und neun Antragsverfahren. Das Projekt befindet sich derzeit noch in der Optimierungsphase, die eigentliche Projektarbeit beginnt erst mit der Prüfung der Optimierungsvorschläge. Dabei wird darauf zu achten sein, dass eine Vorratsdatenspeicherung, wie sie ELENA von Kritikern vorgeworfen wurde, ausgeschlossen ist.

Bea so gut wie abgeschlossen

Das Projekt Bea des Bundesministeriums für Arbeit und Soziales (BMAS) bezieht sich ausschließlich auf die Bescheinigungen (Arbeits-, Nebeneinkommens- und Arbeitsbescheinigungen des über- und zwischenstaatlichen Rechts) zwischen den Arbeitgebern und den Agenturen für Arbeit. Es ist so gut wie abgeschlossen. Ein Referentenentwurf steht noch aus. Ein entscheidender Punkt wird die Wahlmöglichkeit des Arbeitgebers sein, zu entscheiden, ob er die Arbeitsbescheinigung weiterhin über das überarbeitete Papierformular oder elektronisch an die Bundesagentur für Arbeit (BA) übermitteln möchte. Im Gegensatz zum ELENA-Verfahren, in dem immer der Arbeitgeber der zentralen Stelle melden sollte, soll in Bea nur noch auf Verlangen des Arbeitnehmers oder bei einem Leistungsantrag eine Übermittlung der Meldung des Arbeitgebers an die Agentur für Arbeit vorgenommen werden. Nach Eingang der elektronischen Übermittlung der Arbeitsbescheinigung bei der Agentur für Arbeit erhält der Arbeitnehmer einen Ausdruck, so dass der Arbeitnehmer fehlerhafte Einträge noch vor der Leistungsentscheidung korrigieren kann.

Aufgrund datenschutzrechtlicher Bedenken ist bei Vorliegen von vertragswidrigem Verhalten nur noch eine allgemeine Information an die BA zu geben. Es werden keine konkreten Angaben zu dem Fehlverhalten des Arbeitnehmers auf der Bescheinigung eingetragen. Falls vertragswidrige Gründe vorgelegen haben, werden diese Gründe, soweit für die Leistungsgewährung notwendig (Beurteilung einer möglichen Sperrzeit, in der kein Anspruch auf Arbeitslosengeld besteht) von der BA bei dem Arbeitnehmer und Arbeitgeber in einem zusätzlichen Verfahren erfragt. Die übermittelte Arbeitsbescheinigung kann nur von dem zuständigen Mitarbeiter bei der Agentur für Arbeit eingesehen und bearbeitet werden.

Aufgrund datenschutzrechtlicher Bedenken ist bei Vorliegen von vertragswidrigem Verhalten nur noch eine allgemeine Information an die BA zu geben.

Das BMAS plant, die Änderungen des SGB III, die sich durch das Projekt Bea ergeben, noch in dieser Legislaturperiode abzuschließen.

Mitgliederwerbung: Keine Meldedaten für Musikschulen, Vereine und Verbände

Im Rahmen einer Eingabe teilte ein Vater mit, dass sein Kind von einer Musikschule angeschrieben und auf deren Musikschulangebot hingewiesen worden sei. Die personenbezogenen Daten des Kindes hatte die Musikschule im Rahmen einer so genannten Gruppenauskunft auf Antrag von der Meldestelle erhalten, wie dem Vater auf Rückfrage mitgeteilt wurde.

In Übereinstimmung mit den rahmenrechtlichen Vorgaben des § 21 Abs. 3 S. 1 Melderechtsrahmengesetzes (MRRG) bestimmt § 33 Abs. 5 S. 1 Niedersächsisches Meldegesetz (NMG), dass eine Gruppenauskunft (Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Personen) nur erteilt werden darf, soweit sie im öffentlichen Interesse liegt. Eine Gruppenauskunft darf jedoch nicht erteilt werden, wenn der verfolgte Zweck zwar im öffentlichen Interesse liegt, aber auch auf andere Weise ohne Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen erreicht werden kann, etwa durch öffentliche Aufrufe, Zeitungsanzeigen oder Postwurfsendungen. Auf diese Weise werden Musikschulen, Vereine und Verbände regelmäßig erfolgreich Mitglieder gewinnen können.
Die Gruppenauskunft kommt also nur in Betracht, wenn begründet werden kann, dass auf diese Weise Mitglieder nicht erfolgreich gewonnen werden können. Als weitere Voraussetzung einer Gruppenauskunft muss dann das öffentliche Interesse vorliegen.

Werbezwecke stellen kein öffentliches Interesse dar

Die Gruppenauskunft kommt also nur in Betracht, wenn begründet werden kann, dass auf diese Weise Mitglieder nicht erfolgreich gewonnen werden können. Als weitere Voraussetzung einer Gruppenauskunft muss dann das öffentliche Interesse vorliegen.

Die Meldestelle der betroffenen Kommune vertrat die Auffassung, die entsprechende Gruppenauskunft an die Musikschule liege im öffentlichen Interesse, da die Einbindung möglichst vieler Kinder in ein pädagogisches Gesamtkonzept zur frühkindlichen musikalischen Erziehung im Rahmen des Bildungsauftrages der öffentlichen Hand erfolge und gesellschaftlichen sowie kulturellen Interessen diene. Daneben handele es sich bei der konkreten Musikschule um eine Einrichtung in Form einer gemeinnützigen Gesellschaft, die keine kommerziellen Interessen verfolge.
Sowohl aus melderechtlicher als auch aus datenschutzrechtlicher Sicht ist unter dem Begriff des öffentlichen Interesses in erster Linie das Interesse der Allgemeinheit zu verstehen, das sich vom Individualinteresse einzelner Personen oder Gruppen grundsätzlich unterscheidet und über das berechtigte Interesse einzelner Auskunftssuchender hinausgeht. Bei der Prüfung des Vorliegens des öffentlichen Interesses ist auf die konkreten Zwecke, denen die Auskunft die-

nen soll, und die beabsichtigte Art der Verwendung der Daten abzustellen. Rein kommerzielle Interessen (zum Beispiel Werbezwecke) stellen kein öffentliches Interesse dar. Die Mitgliederwerbung von Vereinen und Verbänden, auch wenn diese gesellschaftliche und/oder kulturelle Bedeutung haben, liegt nicht im öffentlichen, sondern allein im Interesse der Organisation. Dieses gilt selbst in den Fällen, in denen eine Organisation gemeinnützige Zwecke verfolgt, deren Unterstützung im öffentlichen Interesse liegt.

Auch Musikschulen nehmen im weitesten Sinne am Wettbewerb teil, selbst wenn diese gemeinnützig tätig sind und ein Gewinnstreben nicht im Vordergrund steht, und das Angebot nur auf eine (befristete) Benutzung der Musikschule ausgerichtet ist. Durch das Anschreiben der Kinder findet dennoch eine Kundenwerbung statt. Zwar ist die Gefahr des Missbrauchs der Daten einer Sammelauskunft bei einer allein durch die öffentlichen Hand getragenen Musikschule geringer als bei einem privaten Verein, dennoch sind den Betroffenen, deren Daten durch die Meldestelle übermittelt werden, etwaige Unterschiede zwischen einer Musikschule in öffentlich-rechtlicher Trägerschaft und privaten Musikschulen oder Vereinen kaum zu vermitteln.

Durch das Anschreiben der Kinder findet eine Kundenwerbung statt.

Ebenso zielen Sportvereine mit einer Mitgliederwerbung auf eine längerfristige Bindung des Mitglieds an den Verein und die Eingehung entsprechender (vereinsrechtlicher) Rechte und Pflichten ab, daher liegt auch für die Erteilung von Gruppenauskünften an Sportvereine zum Zwecke der Mitgliederwerbung kein öffentliches Interesse vor.

Bundesmeldegesetz: Nach viel Kritik Kompromiss im Vermittlungsausschuss

Im Zuge der Föderalismusreform wurde das Meldewesen in die ausschließliche Gesetzgebungskompetenz des Bundes überführt. Mit dem Inkrafttreten eines Gesetzes zur Fortentwicklung des Meldewesens wird das neue Bundesgesetz die bis dahin geltenden einzelnen Landesmeldegesetze der einzelnen Bundesländer ersetzen. Der Referentenentwurf lag dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und den Landesbeauftragten für den Datenschutz vor und wurde gemeinsam behandelt.

In einer abgestimmten Stellungnahme des BfDI und der Landesbeauftragten für den Datenschutz vom 28.6.2011 wurden vom BfDI gegenüber dem Bundesinnenministerium die Aspekte dargelegt, die aus datenschutzrechtlicher Sicht noch zu berücksichtigen sind, da der Regierungsentwurf zum Teil hinter dem bereits geltenden Recht zurückblieb. Daraufhin erstellte die Bundesregierung im November 2011 einen weiteren Gesetzesentwurf (Deutscher Bundestag, Drucksache 17/7746), der im April 2012 erstmals im Bundestag beraten und zur Beratung an die Fachausschüsse überwiesen wurde.
Der Bundestag beschloss daraufhin in der zweiten und dritten Lesung am 28.6.2012 überraschend ein neues „Gesetz zur Fortentwicklung des Meldewesens“, das unscheinbare Änderungen zum Gesetzesentwurf enthielt, die jedoch gravierende Konsequenzen für die betroffenen Bürgerinnen und Bürger und die Kommunen mit ihren Meldebehörden darstellen würden. Dass der geänderte Gesetzesentwurf innerhalb weniger Minuten von nur wenigen anwesenden Bundestagsabgeordneten beschlossen wurde, während parallel im Fernsehen das Halbfinale Deutschland – Italien der Fußball-EM übertragen wurde, führte zu öffentlicher Erregung in Presse und Fernsehen, da der Eindruck entstand, das neue Gesetz sei in einer Nacht- und Nebelaktion an der Öffentlichkeit vorbei unbemerkt durchgewinkt worden.

Bundestag begünstigt Adresshandel

Der Streit entzündete sich an der Frage, unter welchen Bedingungen Meldedaten von den Meldestellen an Dritte übermittelt werden dürfen, wenn die Daten für Werbung oder den Handel mit Adressen verwendet werden sollen. In dem ursprünglichen Referentenentwurf vom 16.3.2011 durften Meldedaten für Zwecke der Werbung und des Adresshandels nicht verwendet werden, „es sei denn, die betroffene Person hat in die Übermittlung eingewilligt“. Aus dieser vorgesehenen Einwilligungslösung wurde dann jedoch in der verabschiedeten Gesetzesfassung auf einmal eine Widerspruchslösung. Darüber hinaus entfaltete nach dem neuen Gesetz auch der Widerspruch keine Wir-

kung, wenn die Daten „ausschließlich zur Bestätigung oder Berichtigung bereits vorhandener Daten verwendet werden". Somit könnte jede Firma, die Daten von Personen erfasst hat, sich diese von der Meldestelle bestätigen oder berichtigen lassen, unabhängig davon, ob nunmehr ein Widerspruch der betroffenen Person vorliegt oder nicht. Da die Meldestellen für derartige Melderegisterauskünfte Gebühren erheben, entstand zudem in der Öffentlichkeit der Eindruck, dass die Kommunen in Zukunft der Wirtschaft zuarbeiteten, da mit den Melderegisterauskünften Geld zu verdienen sei.

Konferenz der Datenschutzbeauftragten fordert Bundesrat auf, dem Gesetz nicht zuzustimmen

Weil das im Bundestag beschlossene neue Meldegesetz auch insgesamt datenschutzrechtliche Verschlechterungen erfahren hatte und die in der gemeinsamen Stellungnahme von BfDI und den Landesdatenschutzbeauftragten vom 28.6.2011 erhobenen Forderungen nicht berücksichtigt worden waren, fasste die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 22.8.2012 die Entschließung „Melderecht datenschutzkonform gestalten!" Mit der Entschließung forderten die Datenschutzbeauftragten den Bundesrat auf, dem Gesetz zur Fortentwicklung des Meldewesens nicht zuzustimmen, damit im Vermittlungsverfahren die Datenschutzdefizite des Bundesmeldegesetzes beseitigt werden können.

Vermittlungsausschuss beschließt Datenweitergabe zu Werbezwecken nur bei Einwilligung

Der Bundesrat beschloss daraufhin in seiner Sitzung am 21.9.2012 die Anrufung des Vermittlungsausschusses, der im Februar 2013 einen Kompromiss fand. Dieser sieht vor, dass Namen und Anschriften aus den Melderegistern von den Einwohnermeldeämtern nur noch zu Werbezwecken an Firmen weitergegeben werden dürfen, wenn die Betroffenen (also die im Melderegister gespeicherten Personen) ausdrücklich vorher zugestimmt haben.

Dazu sollen sie entweder ihre generelle Zustimmung bei der Meldebehörde erklären, oder aber das Unternehmen, das die Daten nutzen will, holt das Einverständnis der Betroffenen ein. Um die Bürger vor Schattenmelderegistern und „Adresspooling" zu schützen, dürfen übermittelte Meldedaten von den Empfängern künftig auch nur noch für den konkreten und übermittelten Zweck verwendet werden und sind anschließend zu löschen.

Weitere Informationen:

Bundestagsdrucksache 17/10768 unter
www.bundestag.de/dokumente/drucksachen

Entschließungen der Konferenz der Datenschutzbeauftragten
www.lfd.niedersachsen.de >Allgemein >DSB-Konferenzen >Entschließungen

Hartz IV: Optionskommunen fast ohne Mängel

Im Volksmund werden die Leistungen der Grundsicherung für Arbeitslose nach dem Sozialgesetzbuch – Zweites Buch (SGB II) gerne als Hartz IV bezeichnet. Das Arbeitslosengeld II wird entweder von der Bundesagentur für Arbeit und dem jeweiligen kommunalen Leistungsträger als gemeinsame Einrichtung gezahlt, oder die Kommune ist als so genannte Optionskommune alleiniger zugelassener Träger dieser Leistungen.

Im Bereich des SGB II obliegt mir die datenschutzrechtliche Aufsicht über die Optionskommunen. Die gemeinsamen Einrichtungen werden hingegen vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontrolliert. Zum 1.1.2012 wurde die Liste der zugelassenen kommunalen Träger um die vier Landkreise Aurich, Friesland, Schaumburg und Wittmund erweitert. In Niedersachsen gibt es nunmehr 17 Landkreise, welche nach diesem Modell die Aufgaben nach dem SGB II übernehmen und über 85.000 Bedarfsgemeinschaften betreuen. Damit liegt Niedersachsen bundesweit auf dem zweiten Platz hinter Nordrhein-Westfalen mit 18 Optionskommunen.

Die Erweiterung der Zahl der Optionskommunen hat zu einem spürbaren Anstieg der Eingaben geführt. Auch wenn die Mehrzahl der Eingaben keinen Anlass zu Beanstandungen gab, habe ich im Jahr 2012 veranlasst, jeder dieser Kommunen einen Besuch abzustatten. Im Vorfeld der Besuche haben sich meine Mitarbeiterinnen und Mitarbeiter mit den Kolleginnen und Kollegen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Bonn ausgetauscht, da diese bereits über Erfahrungen im Bereich der Prüfung von Jobcentern verfügen.

Mittels eines 52 Punkte umfassenden Fragebogens, persönlicher Gespräche mit Landräten, Behördenleitern, Teamleitern der Fachbereiche Soziales, IT-Verantwort-

lichen und mit behördlichen Datenschutzbeauftragten sowie einer Begehung der Räumlichkeiten gelang es, das Verständnis für den Datenschutz zu schärfen. Die Gespräche waren allesamt sehr konstruktiv, und es wurde deutlich, dass durchweg ein großes Interesse an der Verbesserung des Datenschutzniveaus besteht.
Bei den Begehungen wurde der Focus auf die Räumlichkeiten gelegt, welche die Kunden vom Empfang bis zu den Arbeitsvermittlern aufsuchen. Schwere, offensichtliche Datenschutzverstöße wurden in keiner der 17 Optionskommunen festgestellt, wobei aus zeitlichen Gründen eine Prüfung von Aktenvorgängen, Vordrucken und Softwareprogrammen unterbleiben musste. Bei den Rundgängen sind verschiedene Kleinigkeiten aufgefallen, zu denen Anregungen für datenschutzgerechtere Änderungen gegeben wurden. Vorgeschlagen wurde zum Beispiel

- einen Mülleimer neben einem Kopierer zu entfernen, weil Fehlkopien mitgenommen oder geschreddert werden müssen,
- im Wartebereich einen Platz einzurichten, an dem Bürgerinnen und Bürger vor fremden Augen geschützt Anträge ausfüllen können,
- die Diskretionszone am Empfang durch Schilder und Stellwände klar abzugrenzen.

Die Vorschläge meiner Mitarbeiterinnen und Mitarbeiter wurden zum Teil sofort umgesetzt, oder es wurde zugesagt, die Änderungen baldmöglichst vorzunehmen. Die Optionskommunen in Niedersachsen sind zumindest hinsichtlich der räumlichen Ausstattung datenschutzrechtlich bereits gut aufgestellt. Dazu mag die Arbeit der behördlichen Datenschutzbeauftragten vor Ort beigetragen haben, die allerdings viel zu wenig Zeitanteile für ihre Tätigkeit als Datenschutzbeauftragte zugebilligt bekommen. Es ist leider häufig noch so, dass die Aufgabe der oder des behördlichen Datenschutzbeauftragten eine zusätzliche Nebentätigkeit darstellt, wobei die anfallenden Mehrbelastungen nicht voll ausgeglichen werden. Hier ist es aus meiner Sicht erforderlich, den Kommunen entsprechende Haushaltsmittel zur Verfügung zu stellen.

zensus 2011
Wissen, was morgen zählt

Zensus 2011:
Weitgehend datenschutzgerecht

Bereits in meinem XX. Tätigkeitsbericht (S. 17 ff.) bin ich ausführlich auf den Zensus 2011 eingegangen und habe die Grundlagen dargelegt. Europaweit stattgefunden hat der Zensus 2011, die sogenannte Volkszählung, zum Stichtag 9. Mai 2011. An diesem Tag begannen die Befragungen. Sie erfolgten bei allen Immobilieneigentümern, in Deutschland 2,3 Millionen, im Rahmen einer Gebäude- und Wohnungszählung sowie bei knapp zehn Prozent der Bevölkerung (813.000 Personen) im Rahmen der Haushaltebefragung auf Stichprobenbasis und in sogenannten Sonderbereichen, d. h. unter anderem in Gemeinschafts-, Anstalts- und Notunterkünften und Wohnheimen.

Zu Beginn der Befragung haben sich zahlreiche Bürgerinnen und Bürger schriftlich und telefonisch mit Eingaben und Anfragen an mich gewandt. Sie wollten zum Beispiel wissen, ob eine Auskunftspflicht besteht. Diese Schreiben habe ich individuell beantwortet. Zusätzlich habe ich diese und weitere Informationen in einem Artikel auf meiner Homepage veröffentlicht, in dem ich auch auf die FAQ (Frequently Asked Questions – häufig gestellte Fragen) des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein hingewiesen sowie weitere interessante Links angeführt habe.
Ein anderes Problem zeigte sich Mitte 2011. Zu diesem Zeitpunkt beschwerten sich zahlreiche Auskunftspflichtige bei mir, weil sie Erinnerungsschreiben des Landesbetriebs für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) trotz ordnungsgemäß erteilter Auskunft erhalten hatten. Sie befürchteten einen unzulässigen Umgang mit personenbezogenen Daten. In diesem wie auch in einigen anderen Fällen bat ich das LSKN um Stellungnahme. Ein Verstoß gegen datenschutzrechtliche Vorschriften ließ sich jedoch nicht feststellen.
Die Befragungen waren bis zum Juli 2012 abgeschlossen. Voraussichtlich im Mai/Juni 2013 werden die Statistischen Ämter des Bundes und der Länder die Einwohnerzahlen für Bund, Länder und Kommunen, die Ergebnisse aus der Gebäude- und Wohnungszählung sowie erste Ergebnisse aus der Haushaltebefragung veröffentlichen.

Land setzt neues Verfahren ein:
Viele Schülerdaten für höhere Berufswahlkompetenz

Im Juli 2011 trat das Niedersächsische Kultusministerium an mich heran und bat mich um datenschutzrechtliche Beratung zum Einsatz eines neuen computergestützten Verfahrens zur Steigerung der beruflichen Ausbildungsfähigkeit und Berufswahlkompetenz der Schülerinnen und Schüler. Dieses Verfahren sollte bereits im Schuljahr 2011/2012 eingesetzt und nach einer Probephase landesweit zur Ermittlung der persönlichen Stärken und Entwicklungspotenziale von Jugendlichen im 8. Schuljahrgang an allen Hauptschulen, Realschulen, den entsprechenden Zweigen der Kooperativen Gesamtschulen, den Oberschulen und den Förderschulen Lernen eingeführt werden.

Mit diesem sogenannten Kompetenzfestellungsverfahren werden personenbezogene Daten der Schülerinnen und Schüler verarbeitet. Es ist daher zu prüfen, welche technischen und organisatorischen Maßnahmen nach § 7 Niedersächsisches Datenschutzgesetz (NDSG) zu treffen sind, um eine datenschutzgerechte Verarbeitung dieser Daten sicherzustellen. Gegebenenfalls ist auch eine Vorabkontrolle nach § 7 Abs. 3 NDSG durchzuführen, wenn die Art der zu verarbeitenden Daten oder die Verwendung neuer Technologien besondere Risiken in sich tragen. Außerdem ist jede Stelle, die Verfahren zur automatisierten Verarbeitung personenbezogener Daten einrichtet oder ändert, verpflichtet, eine Verfahrensbeschreibung nach § 8 NDSG zu erstellen.
Ich empfahl dem Kultusministerium, vor Einsatz des Kompetenzfeststellungsverfahrens mindestens ein Datensicherungskonzept aus technischen und organisatorischen Maßnahmen zu erstellen, das in seiner Gesamtheit einen hinreichenden Schutz der Daten vor unsachgemäßer Handhabung gewährleistet. Außerdem sollte das Ministerium, da es den Schulen dieses Verfahren vorgibt, eine Muster-Verfahrensbeschreibung erstellen und den Schulen zur Verfügung stellen. Letzteres ist geschehen.
Leider musste ich feststellen, dass viele Schulen die Erstellung einer Verfahrensbeschreibung als „bürokratisches Hemmnis“ sehen, aber nicht die Bedeutung erkennen. So füllen sie zwar die Verfahrensbeschreibung aus, übernehmen jedoch lediglich die Angaben aus der Muster-Verfahrensbeschreibung und passen diese nicht an die besonderen Gegebenheiten der jeweiligen Schule vor Ort an. Ich habe das Kultusministerium gebeten, die Schulen auf die individuelle Anpassung der Verfahrensbeschreibungen hinzuweisen.

Medienkompetenz:
Datenschutz als Bildungsaufgabe

Die Entwicklung und Stärkung der Medienkompetenz betrifft jeden und ist eine gesamtgesellschaftliche Aufgabe. Aus diesem Grunde beschäftigen sich die unterschiedlichsten Stellen mit diesem Thema. Auch ich bin bereits in meinem XIX. und XX. Tätigkeitsbericht (S. 10 bzw. 16) darauf eingegangen. In diesem Bericht werde ich mich ausschließlich auf den Bereich der Medienkompetenz bei Schülerinnen und Schülern beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im September 2011 eine Entschließung mit dem Titel „Datenschutz als Bildungsaufgabe" verabschiedet, in der sie unter anderem fordert, dass

- sich die schulischen Programme und Projekte zur Medienkompetenz nicht auf Fragen des Jugendmedienschutzes und des Urheberrechts beschränken, sondern den Datenschutz als wesentlichen Bestandteil mit einbeziehen, und
- Medien- und Datenschutzkompetenz entweder in einem eigenständigen Schulfach oder in einem Fächerspektrum mit Leitfächern verpflichtend zu verankern sind und zum Gegenstand der Lehrerausbildung gemacht werden.

Die Niedersächsische Landesregierung hat diese Forderungen in ihr Konzept „Medienkompetenz in Niedersachsen – Meilensteine zum Ziel" übernommen, das sie am 14.2.2012 beschlossen hat. Das Konzept, das sich auf die Bereiche:

- Schulen, Kindertagesstätten, Lehreraus- und -fortbildung,
- Familien/Jugendarbeit/Jugendschutz sowie
- Hochschule und Weiterbildung

konzentriert, betont unter anderem, dass die Vermittlung von Medienkompetenz praktizierter präventiver Jugendschutz ist und in engem Zusammenhang mit Zielen des Verbraucherschutzes, des Datenschutzes und der Kriminalprävention steht. Es geht auf die Notwendigkeit ein, den Datenschutz schon bei der Ausbildung der Lehrkräfte im Studienseminar zu thematisieren und weist auf den Selbstdatenschutz hin.
Die Kultusministerkonferenz hat sich ebenfalls diesem Thema gewidmet und am 8.3.2012 den Beschluss zur „Medienbildung in der Schule" gefasst. Darin wird neben der Medienbildung in der Schule auf die Kooperation mit außerschulischen Institutionen wie den Landesbeauftragten für den Datenschutz hingewiesen. Im Sommer 2012 stellte die Niedersächsische Landesmedienanstalt auf ihrer Homepage kostenfrei Unterrichtsmaterialien zu den Themen Internet, Handy, Computerspiele & Co bereit, die insbesondere auf den Einsatz in den Klassenstufen 7 und 8 an Haupt- und Realschulen ausgerichtet sind.
In meinen Beratungen und Fortbildungen weise ich auf die zu diesem Themenbereich erstellten Materialien hin und erwähne insbesondere die bereits im XX. Tätigkeitsbericht aufgeführte Linkliste des Arbeitskreises Datenschutz und Bildung der Datenschutzbeauftragten des Bundes und der Länder mit dem Themenschwerpunkt Medienkompetenz und Datenschutz, die regelmäßig aktualisiert wird.

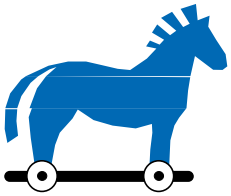
Weitere Informationen:

Entschließungen der Konferenz der Datenschutzbeauftragten:
www.lfd.niedersachsen.de >Allgemein >DSB-Konferenzen >Entschließungen

Beschluss der Landesregierung:
www.medienkompetenz-niedersachsen.de

Beschluss der Kultusministerkonferenz:
www.kmk.org/fileadmin/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf

Linkliste Arbeitskreis Datenschutz und Bildung:
www.datenschutz.rlp.de/de/linkliste_ag_schule.php



Vervielfältigen von Lehrmaterial: Es geht auch ohne „Schultrojaner“

Die Bundesländer schlossen am 21.12.2010, weitgehend unbeachtet von der Öffentlichkeit, mit der Verwertungsgesellschaft Wort, der Verwertungsgesellschaft Musikedition und verschiedenen Schulbuchverlagen einen Gesamtvertrag zur Einräumung und Vergütung von Ansprüchen nach § 53 Urheberrechtsgesetz. Hauptbestandteil dieses Vertrages ist eine pauschale Vergütung für das Vervielfältigen von Lehrmaterial. Erst Ende Oktober 2011 sorgte eine laut Vertrag vorgesehene Plagiatssoftware für große Aufregung.

Wörtlich hieß es dazu im Vertrag: „Die Verlage stellen den Schulaufwandsträgern sowie den kommunalen und privaten Schulträgern auf eigene Kosten eine Plagiatssoftware zur Verfügung, mit welcher digitale Kopien von für den Unterrichtsgebrauch an Schulen bestimmten Werken auf Speichersystemen identifiziert werden können. Die Länder wirken – die technische und datenschutzrechtliche Unbedenklichkeit der Software vorausgesetzt – darauf hin, dass jährlich mindestens 1 % der öffentlichen Schulen ihre Speichersysteme durch Einsatz dieser Plagiatssoftware auf das Vorhandensein solcher Digitalisate prüfen lässt.“
Die Medien berichteten über den „Schultrojaner“, der Niedersächsische Landtag befasste sich mit dem Thema, und mich erreichten zahlreiche Anfragen, so dass ich das Niedersächsische Kultusministerium um Stellungnahme bat. Bevor jedoch dessen Antwort vorlag, teilte bereits die Kultusministerkonferenz in einer Pressemitteilung am 13.12.2011 folgendes mit:

„Die in § 6 Abs. 4 des Vertrages beschriebene ‚Scansoftware’ wird nach Einschätzung der Vertragspartner bis auf Weiteres, jedenfalls nicht im Jahr 2012, zum Einsatz kommen. Die Vertragspartner verabredeten, im ersten Quartal 2012 ein weiteres Gespräch zu führen, um mögliche Alternativen zu diskutieren. Alle Gesprächsteilnehmer waren sich einig, dass das geistige Eigentum zu schützen sei und die Rechte der Verlage und Autoren, vor allem auch der beteiligten Lehrkräfte, gewahrt werden müssen. Die Lehrerverbände werden weiter in die Gespräche einbezogen.“

Nachdem weitere Verhandlungen der Länder mit den Verlagen erfolgten, teilte am 4.5.2012 das für die Länder federführende Bayerische Staatsministerium für Unterricht und Kultus mit, dass bundesweit vom Einsatz einer Plagiatsoftware abgesehen werde. Damit hatte sich die Entwicklung einer Plagiatssoftware erledigt. Aus einer Pressemitteilung der Kultusministerkonferenz vom 6.12.2012 erfuhr ich, dass die Vertragsparteien einen neuen Urheberrechtsvertrag geschlossen haben, der ohne den Einsatz einer Plagiatssoftware auskommt und in dem neben der Genehmigung zum Anfertigen von Kopien in Papierform auch das digitale Vervielfältigen im begrenzten Umfang erlaubt ist.

2 Datenschutz in der Wirtschaft

Beschäftigtendatenschutz: Das Provisorium lebt, neues Gesetz nicht in Sicht

In meinem letzten Tätigkeitsbericht hatte ich dargestellt, dass die Regelungen zum Beschäftigtendatenschutz in Bewegung sind: Zum 1. September 2009 wurde in das Bundesdatenschutzgesetz mit § 32 eine gesonderte Regelung zum Beschäftigtendatenschutz eingefügt. Die neue Bundesregierung brachte dann im August 2010 einen Gesetzesentwurf zum Beschäftigtendatenschutz in den Bundestag ein.

Nach diesem Entwurf sollte ein eigener Unterabschnitt im Bundesdatenschutzgesetz die Datennutzung im Beschäftigtenverhältnis regeln. Über zwei Jahre lang befand sich der Entwurf im Gesetzgebungsverfahren, ohne dass außerhalb des parlamentarischen Verfahrens ein nennenswerter Fortgang erkennbar gewesen wäre. Anfang 2013 kam plötzlich wieder Bewegung in die Angelegenheit, als die Koalitionsfraktionen den ursprünglichen Regierungsentwurf aufgriffen und hierzu zugleich einen umfassenden Änderungsentwurf in den Innenausschuss des Bundestages einbrachten. Zwar ist es zugegebenermaßen schwierig, auf dem sensiblen Feld des Beschäftigtendatenschutzes allen mitunter gegenläufigen Interessen gerecht zu werden. Allerdings enthielt der von den Koalitionsfraktionen vorgelegte Entwurf etliche Regelungen, die im Vergleich zum ursprünglichen Regierungsentwurf das Niveau des Beschäftigtendatenschutzes noch weiter abgesenkt hätten.
Dies hob die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 25.1.2013 hervor. Darin wurde insbesondere kritisiert, dass der Gesetzesentwurf die Möglichkeiten der offenen Videoüberwachung am Arbeitsplatz massiv ausweite und die Möglichkeit schaffe, die Mitarbeiter in Callcentern einer stärkeren Telefonüberwachung auszusetzen; hierdurch entstünde ein unzumutbarer Überwachungsdruck. Zugleich gab es auf Arbeitnehmerseite einen nicht unerheblichen öffentlichen Proteststurm gegen den Gesetzesentwurf. So sammelte der DGB in einer Online-Petition nach eigenen Angaben mehr als 30.000 Unterschriften gegen das Vorhaben. Hierbei kritisierte der DGB unter anderem die im Gesetzentwurf vorgesehene Privilegierung der Datenweitergabe innerhalb eines Konzernverbundes.
Die Kritik zeigte Wirkung. Ende Januar 2013 wurde das Thema von der Tagesordnung des Innenausschusses sowie des Bundestages genommen. Zugleich wurde deutlich, dass innerhalb der laufenden Legislaturperiode kein entsprechendes Gesetz mehr verabschiedet wird.
Auf ausgewogene Detailregelungen zum Beschäftigtendatenschutz muss also weiter gewartet werden. Es verbleibt daher bei dem ursprünglich als Provisorium gedachten § 32 BDSG.

Weitere Informationen:

Entschließungen der Konferenz der Datenschutzbeauftragten:
www.lfd.niedersachsen.de
>Allgemein >DSB-Konferenzen >Entschließungen

Meldepflicht bei Datenpannen: Reaktion nicht immer unverzüglich

Mit Wirkung vom 1.9.2009 trat § 42a Bundesdatenschutzgesetz (BDSG) in Kraft. Diese Regelung wurde geschaffen, weil in der Vergangenheit häufiger Datenpannen mit erheblichen Auswirkungen für die Betroffenen eingetreten waren. Die Unternehmen sind nunmehr verpflichtet, solche Datenpannen den Aufsichtsbehörden und den Betroffenen unverzüglich mitzuteilen.

Im Bereich der Kreditwirtschaft sind Datenverluste und mögliche unrechtmäßige Kenntnisnahmen von Daten regelmäßig nach § 42a BDSG zu melden, da überwiegend auch Konto- und Kreditkartendaten betroffen sind. Die Pflicht zur Information des Betroffenen wird jedoch nur ausgelöst, wenn zusätzlich schwerwiegende Beeinträchtigungen für seine Rechte oder schutzwürdigen Interessen drohen. Daher ist jeder Einzelfall sorgfältig zu prüfen.

Im Berichtszeitraum wurden mir zwei Fälle aus dem besonders sensiblen Bereich der Finanzwirtschaft bekannt, bei denen eingehend geprüft und gewürdigt werden musste, ob die verantwortliche Stelle unverzüglich ihrer Meldepflicht nachgekommen war. In einem Fall hatte eine Bank eine Filiale geschlossen und alle vorhandenen Unterlagen abtransportieren lassen. Das Mobiliar wurde nicht demontiert, da es mit dem Gebäude verkauft worden war, und bei mehreren Sichtkontrollen wurden keinerlei Unterlagen aufgefunden. Nach Überlassung der Räumlichkeiten und des Inventars wurde bekannt, dass der neue Eigentümer Bank- und Kundenbelege in Besitz habe. Nach diversem Schriftverkehr klagte das Geldinstitut gegen den Datenbesitzer auf Auskunfterteilung und Herausgabe der vorhandenen Unterlagen. Die Klage wurde zugunsten des Klägers entschieden. Somit konnte erst etwa zehn Monate nach Datenverlust festgestellt werden, dass es sich um Daten gemäß § 42a BDSG handelte und auch die weiteren Tatbestandsmerkmale erfüllt waren. Es folgten die telefonische und die schriftliche Meldung an die Datenschutzaufsichtsbehörde sowie die schriftliche Benachrichtigung der Betroffenen. Die eingehende Prüfung des Sachverhalts ergab, dass in diesem atypischen Fall die Meldung unverzüglich und die Benachrichtigung der Betroffenen rechtzeitig und vollständig erfolgt war. Die möglichen schwerwiegenden Beeinträchtigungen für die Betroffenen hatte die Bank zutreffend gewichtet, und die Maßnahmen zur Verhinderung künftiger ähnlicher Vorfälle waren angemessen, aber auch erforderlich.

In einem weiteren Fall wurde bei internen Kontrollen festgestellt, dass ein Mitarbeiter eines Geldinstituts unberechtigt Daten seiner Exfrau und seines volljährigen Sohnes abgefragt hatte. Die Sperrung des IT-Zugriffs für den Mitarbeiter erfolgte unverzüglich. Die interne Aufklärung für den genauen Datenzugriff dauerte allerdings sechs Wochen; nach weiteren vier Wochen wurden die Betroffenen und die Aufsichtsbehörde informiert. Da in diesem Fall für vertragliche Zwecke nicht erforderliche Kontobewegungsdaten über einen längeren Zeitraum von einem nicht berechtigten Mitarbeiter erhoben worden waren und auch eine erhebliche Beein-

trächtigung der schutzwürdigen Interessen befürchtet werden musste, war auch in diesem Fall eine Meldung nach § 42a BDSG erforderlich. Gegen den Mitarbeiter wurde neben arbeitsrechtlichen Maßnahmen ein Ordnungswidrigkeitenverfahren eingeleitet. Aus Ermessensgründen sah ich von der Einleitung eines Ordnungswidrigkeitenverfahrens gegen das Unternehmen wegen nicht unverzüglicher Meldung noch ab, wies das Kreditinstitut jedoch auf die künftige Beachtung einer unverzüglichen Meldung an die Datenschutzaufsichtsbehörde hin.

Prüfschema zur Meldepflicht:

1. Welche Daten sind betroffen?
- besondere Daten § 3 Abs. 9 BDSG,
- Berufsgeheimnis,
- Verdacht auf strafbare Handlungen oder Ordnungswidrigkeiten,
- Bank- oder Kreditkartenkonten.

2. Unrechtmäßige Kenntnis durch Dritte durch
- unrechtmäßige Übermittlung,
- sonstige unrechtmäßige Kenntniserlangung?

3. Drohen dem Betroffenen schwerwiegende Beeinträchtigungen
- seiner Rechte,
- seiner schutzwürdigen Interessen?

Kundenwerbung durch Kunden: Nicht ohne Mitwirkung des Interessenten

Jedes Unternehmen will neue Kunden gewinnen und damit seinen Umsatz und Gewinn steigern. Da in diesem Fall häufig personenbezogene Daten erhoben, gespeichert und verarbeitet werden, gelten auch die Regelungen des Bundesdatenschutzgesetzes (BDSG). Im Berichtszeitraum stellte sich die Frage, ob die Akquise neuer Kunden durch die Aufforderung an die Altkunden, weitere Bekannte zu benennen, datenschutzrechtlich zulässig ist.

Von Seiten der Wirtschaft wird vereinzelt die Auffassung vertreten, dass die Befragung von Kunden über potentielle weitere Interessenten aus dem Bekanntenkreis für eine Beratung eine zulässige Datenerhebung ist. Sie dürfe auch ohne Mitwirkung und Kenntnis des möglichen Interessenten erfolgen. In der Regel werden bei diesem Verfahren zur Kundengewinnung die personenbezogenen Daten möglicher Interessenten beim Altkunden durch einen Handelsvertreter per Notebook erhoben und an die Zentrale zur Direktansprache durch den dafür zuständigen Handelsvertreter übermittelt. Als Aufsichtsbehörde für den Datenschutz in Niedersachsen vertrete ich dagegen eine andere Auffassung. Nach § 3 Abs. 3 BDSG ist das Beschaffen von Daten über Betroffene als Erheben definiert. Unter automatisierter Verarbeitung wird die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen verstanden. Da die Datenerhebung „unter Einsatz von Datenverarbeitungsanlagen“ erfolgt, unterfällt sie (und die gleichzeitige Speicherung) dem Oberbegriff der Verarbeitung.

Nichtkunden müssen in Speicherung einwilligen

Grundsätzlich sind personenbezogene Daten beim Betroffenen zu erheben (§ 4 Abs. 2 BDSG). Ausnahmen sind nur unter strengen Bedingungen zugelassen und unterliegen einer Interessenabwägung. Vor dem Hintergrund des Schutzgedankens des informationellen Selbstbestimmungsrechts und des Transparenzgebots ist zudem im Hinblick auf eine Datenspeicherung ohne Kenntnis des Betroffenen in § 33 Abs. 1 Satz 1 BDSG eine besondere Benachrichtigungsregelung getroffen worden. Spätestens seit der Verschärfung des Gesetzes gegen den unlauteren Wettbewerb (UWG) ist auch die Speicherung von Telefon- und Faxnummern sowie E-Mail-Adressen von Nichtkunden nicht mehr ohne deren Einwilligung zulässig, da diese Daten nicht zur direkten Kundenansprache ge-

nutzt werden dürfen. Eine vorherige Zustimmung des Interessenten für die Datennutzung ist in diesem Verfahren nicht möglich.
Die Daten, die der Altkunde seinem Berater (Handelsvertreter) mitteilt, dienen dazu, dass dieser in Abstimmung mit der Zentrale beim potentiellen Interessenten ein Beratungsgespräch durchführt. Sollte der mögliche Interessent außerhalb des Betreuungsgebietes des Handelsvertreters seinen Wohnsitz haben, werden die Daten von der Zentrale an den entsprechend zuständigen Berater übermittelt. Zweck der Akquisition von Interessentendaten ist die Erstellung einer Datenbank für das Marketing. Marketing und Werbung gehören zu den ureigensten Interessen eines Unternehmens. Der Grund für die Erhebung und Speicherung der Daten ist daher die werbliche Nutzung. Für die Nutzung von Daten zu werblichen Zwecken ist § 28 Abs. 3 BDSG als lex specialis gegenüber § 28 Abs. 1 und 2 BDSG anzuwenden. Die vereinzelt vertretene Auffassung, dass § 28 Abs. 3 BDSG nicht abschließend die Verarbeitung von personenbezogenen Daten zu Werbezwecken regelt, teile ich nicht. Nach allgemeiner mehrheitlicher Meinung in der Literatur wird § 28 Abs. 3 BDSG als eine abschließende Spezialregelung für die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder Werbung angesehen.
§ 28 Abs. 3 Satz 1 BDSG erachtet die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke der Werbung als zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Abs. 3a verfährt. Die Anwendung der Regelungen aus § 28 Abs. 3 Satz 2 Nr. 1 BDSG scheitert bereits an dem Tatbestandsmerkmal der „listenmäßig oder sonst zusammengefassten Daten". Eine listenmäßige Zusammenfassung besteht nicht, wenn nur Daten einer einzigen Person verwendet werden. Im vorliegenden Falle werden die Kontaktdaten jeweils einzelner potentieller Interessenten erhoben und verwendet. Eine listenmäßige Zusammenfassung liegt damit nicht vor. Selbst wenn man § 28 Abs. 3 Satz 2 Nr. 1 BDSG für anwendbar hält, scheitert die weitere Datennutzung für Werbezwecke an der gesetzlich vorgegebenen Regelung der Datenerhebung beim Betroffenen. Der Grundsatz aus § 4 Abs. 2 BDSG wird gerade auch hier in dieser speziellen Regelung für Werbezwecke wiederholt („… die diese Daten … beim Betroffenen … erhoben hat."). Hinzu kommt, dass das Merkmal der Erforderlichkeit (§ 28 Abs. 3 Satz 2 BDSG) nicht gegeben ist, weil es andere Möglichkeiten der Datenerhebung gibt. So sind zum Beispiel die Nutzung von Adressbrokern/Lettershops sowie weitere denkbare Alternativen möglich.

Mit Unterschrift oder per Postkarte

Als rechtlich zulässig könnte ein Verfahren angesehen werden, in dem der Altkunde als Werber seine Daten auf einem Formular mitteilt, auf dem auch der Neukunde mit Unterschrift sein Interesse und seine Daten an ein Unternehmen meldet. Dabei müsste besonders darauf geachtet werden, dass zur Erfüllung des Auskunftsrechts nach § 34 BDSG die Datenherkunft dokumentiert ist. Die Erhebung der Daten eines Interessenten setzt somit voraus, dass dieser selbst seine Daten mitteilt bzw. den Kontakt zu einem Anbieter sucht. Denkbar ist auch, dass zufriedene Kunden eine frankierte Postkarte erhalten, die sie den potentiellen Interessenten aushändigen, damit diese eine Beratung anfordern.

Auch die Ad-hoc-Arbeitsgruppe „Werbung und Adresshandel" der Aufsichtsbehörden für den Datenschutz hat in ihrer Sitzung am 23./24.4.2012 einstimmig das Verfahren der Datenerhebung durch Befragung von Altkunden als unzulässig angesehen.

Antiterrorlisten und Sicherheitsüberprüfungen: Die vergebliche Suche nach Rechtsgrundlagen

Das sogenannte AEO-Zertifikat, das auf Antrag vom Zoll erteilt wird und mit dem Außenwirtschaftsunternehmen in den Genuss vereinfachter, deutlich schnellerer Zollabwicklungen kommen, ist geknüpft an eine Sicherheitsüberprüfung („Screening") der Firmenmitarbeiter. Dies kann als Beispiel dienen zu dem Thema „Wie bringt man mehrere nachvollziehbare Ziele unter einen Hut?" Es kann aber auch als Beispiel dafür dienen, dass es manchmal trotz einer Vielzahl von Rechtsvorschriften nicht gelingt, eine passende Rechtsgrundlage zu finden.

Die exakte Bezeichnung des Zertifikats lautet „Zollrechtliche Vereinfachungen/Sicherheit – AEO-F". Mit dem Zertifikat erhält das Unternehmen den Status „Zugelassener Wirtschaftsbeteiligter" („Authorised Economic Operator – AEO"). Der Vorteil der schnelleren Zollabwicklungen bedeutet einen Zeitvorsprung, der im internationalen Transportgewerbe, in dem es oft um Tag und Stunde der Lieferung geht, einen nicht zu unterschätzenden geldwerten Vorteil darstellt. Somit kann das AEO-Zertifikat im Konkurrenzkampf der Unternehmen zu einem Wettbewerbsvorteil oder – bei seinem Fehlen – zu einem Wettbewerbsnachteil werden. Die Bewilligungsvoraussetzungen für die Erteilung dieses Zertifikats sind in Art. 14 k Zollkodex-Durchführungsverordnung (ZK-DVO) geregelt. Hiernach muss das antragstellende Unternehmen unter anderem nachweisen, dass es seine in sicherheitsrelevanten Bereichen tätigen Mitarbeiter einer Sicherheitsüberprüfung unterzogen hat. Welcher Art diese Sicherheitsüberprüfung zu sein hat, wird in der Vorschrift nicht geregelt. Somit liegt es im pflichtgemäßen Ermessen der Zollverwaltung, zu entscheiden, auf welche Weise die Sicherheitsüberprüfung der Beschäftigten erfolgt.

Ein weites Ermessen der Zollverwaltung

Im Rahmen dieses Ermessens fordert die Zollverwaltung von den antragstellenden Unternehmen einen Abgleich mit den sogenannten Antiterrorlisten, die als Anlagen der EU-Verordnungen 2580/2001 und 881/2002 erlassen worden sind.

Voraussetzung für das AEO-Zertifikat ist eine Sicherheitsüberprüfung der Mitarbeiter einschließlich eines Abgleichs mit den EU-Antiterrorlisten

Die Verordnung 2580/2001 vom 27.12.2001 regelt spezifische Maßnahmen zur Bekämpfung des Terrorismus. Die Verordnung 881/2002 vom 27.5.2002 bezieht sich ausdrücklich auf Personen und Organisationen, die mit Osama bin Laden, dem Al-Quaida-Netzwerk und den Taliban in Verbindung stehen. Zu beiden Verordnungen wurden als Anlagen die bereits erwähnten Antiterrorlisten erlassen, in denen zahlreiche Organisationen und Personen aufgeführt sind, die mit terroristischen Handlungen in Verbindung gebracht werden. Anhand dieser Listen soll das antragstellende Unternehmen – so die Entscheidung der Zollverwaltung – die Sicherheitsüberprüfung seiner Beschäftigten durchführen, um das begehrte AEO-Zertifikat zu erhalten.

Fraglos sind die Ziele, die mit den beiden genannten EU-Verordnungen verfolgt werden, wichtig und nachvollziehbar. Gleichwohl stellen sich im Zusammenhang mit der AEO-Zertifizierung etliche datenschutzrechtliche Fragen, wenn zum Beispiel ein in einem Überseehafen tätiges Unternehmen hunderte Mitarbeiter anhand von Antiterrorlisten screenen soll. Zugleich muss der hohe rechtsstaatliche Standard, der zum Erlass der einschlägigen Antiterrorvorschriften geführt hat,

auch im Rahmen des Mitarbeiterscreenings Anwendung finden. Es bedarf also einer Rechtsgrundlage für das Screening.

Das Bundesdatenschutz als Rechtsgrundlage?

Auf nationaler Ebene regelt § 32 Bundesdatenschutzgesetz (BDSG), unter welchen Voraussetzungen Daten der Beschäftigten vom Arbeitgeber genutzt werden können. Insofern kommt zunächst eine Einwilligung des Beschäftigten in Betracht. Eine wirksame Einwilligung des Beschäftigten ist im Über-/Unterordnungsverhältnis zum Arbeitgeber jedoch rechtlich nicht gegeben, da es ihr an der Freiwilligkeit fehlen würde (§ 4a Abs. 1 BDSG). Dies beruht darauf, dass ein Beschäftigter im Arbeitsverhältnis im Zweifel jeder Datennutzung zustimmen würde, um seinen Arbeitsplatz nicht zu gefährden. Von einer autonomen Entscheidung zur Datennutzung kann somit im Rahmen des Beschäftigungsverhältnisses grundsätzlich keine Rede sein. Damit ist eine Datennutzung im Rahmen des § 32 BDSG nur dann zulässig, soweit es für die Durchführung des Beschäftigungsverhältnisses erforderlich ist. Nicht ausreichend ist, dass die Datennutzung nur in (mittelbarem) Zusammenhang zur Durchführung des Beschäftigungsverhältnisses steht. Ebenso wenig wäre ausreichend, dass die Datennutzung dem Arbeitgeber einen finanziellen Vorteil verschafft. Eine Datenerhebung ist somit dann unzulässig, wenn das Beschäftigungsverhältnis auch ohne diese Datenerhebung durchgeführt werden könnte. So verhält es sich hier.

Das Screening ist für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich – der Mitarbeiter würde auch ohne das AEO-Zertifikat seine Arbeitsleistungen erbringen können.

Das bilaterale Beschäftigungsverhältnis spielt sich allein zwischen dem Beschäftigten und dem Arbeitgeber ab. Der Beschäftigte führt hierbei die arbeitsvertraglich geschuldeten Leistungen aus und erhält dafür sein Gehalt. Insofern „funktioniert" das Beschäftigungsverhältnis auch ohne das Screening des Mitarbeiters. Ob das einzelne Zollgut schneller abgewickelt werden kann, ist allein eine Frage zwischen dem Unternehmen und der Zollverwaltung. Dass das AEO-Zertifikat mittelbar die Wettbewerbssituation des Unternehmens verbessert, ist für die (unmittelbare) Erforderlichkeit der Datennutzung im Rahmen des (bilateralen) Beschäftigungsverhältnisses irrelevant. Aus diesem Grund ist die Datennutzung nicht erforderlich im Sinne des § 32 Abs. 1 S. 1 BDSG. Damit scheidet § 32 BDSG als Rechtsgrundlage aus.

Die Zollkodex-Durchführungsverordnung als Rechtsgrundlage?

Art. 14 k ZK-DVO käme ebenfalls als Rechtsgrundlage in Betracht. Es handelt sich um eine EU-Verordnung, so dass sie, anders als EU-Richtlinien, unmittelbar in jedem Mitgliedsstaat gilt. Allerdings stellt dieser Artikel schon aus dem Grund keine hinreichend bestimmte Rechtsgrundlage für das Screening dar, weil die Vorschrift keine Aussage darüber trifft, auf welche Weise die Sicherheitsüberprüfung erfolgen soll. Beispielsweise käme auch die Vorlage von Führungszeugnissen in Betracht. Diese Entscheidung überlässt die Verordnung den Mitgliedsstaaten. Art. 14 k ZK-DVO bezieht sich also nicht auf die beiden genannten EU-Verordnungen und deren Antiterrorlisten und kann daher auch nicht die Rechtsgrundlage für diesen dezidierten Datenabgleich darstellen. Zudem enthält der Artikel den Passus „soweit gesetzlich zulässig" und macht damit deutlich, dass diese Vorschrift nicht selbst die Rechtsgrundlage darstellt.

Die EU-Antiterrorverordnungen als Rechtsgrundlage?

Bei der Frage nach der Rechtsgrundlage des Screenings könnte weiterhin argumentiert werden, dass die beiden genannten EU-Verordnungen „ohnehin" unmittelbar geltendes Recht darstellen. Sie untersagen, an Organisationen und Personen, die in den Antiterrorlisten aufgeführt sind, direkt oder indirekt Gelder, wie zum Beispiel Gehalt, auszuzahlen. Eine Person, die auf einer der Antiterrorlisten aufgeführt ist, dürfte somit bereits deshalb nicht in einem im Geltungsbereich der EU-Verordnungen tätigen Unternehmen beschäftigt sein. Dieses Zahlungsverbot stellt also unmittelbar geltendes Recht dar, das zudem über das Außenwirtschaftsgesetz (§ 34 AWG) strafrechtlich sanktioniert ist. Ein großes Unternehmen kann das Zahlungsverbot „eigentlich" nur mittels eines Screenings umsetzen. Ein solches Screening würde aber eben allein der Umsetzung des aus den EU-Verordnungen resultierenden Zahlungsverbots dienen; es gäbe keinen (normierten) Bezug zur AEO-Zertifizierung. Die beiden Antiterrorverordnungen können somit allenfalls die Rechtsgrundlage darstellen für ein Screening, das der Umsetzung des Zahlungsverbots dient. Ein Screening, das aber allein der AEO-Zertifizierung dient, kann nicht von der Rechtsgrundlage für das Zahlungsverbot, den Verordnungen, gedeckt sein. Daraus wird deutlich, dass die Einbeziehung der Antiterrorlisten in die AEO-Zertifizierung nicht in einer gesetzlichen Vorschrift geregelt ist, sondern auf einer Entscheidung der Zollverwaltung beruht.

Die EU-Antiterrorverordnungen können nicht die Rechtsgrundlage darstellen für Mitarbeiterscreenings, die nicht dem Zahlungsverbot dienen, sondern zu einem gänzlich anderen Zweck erfolgen.

Argument des BFH nicht nachvollzienbar

Teilweise wird in diesem Zusammenhang auch die Meinung vertreten, dass eine gesetzliche Eingriffsgrundlage entbehrlich sei, weil die AEO-Zertifizierung und damit das Mitarbeiterscreening nicht aufgrund staatlichen Zwanges erfolge, das jeweilige Unternehmen dieses Zertifikat vielmehr freiwillig beantrage. Mit dieser Argumentation hat der Bundesfinanzhof (BFH) in einem Urteil vom 19.6.2012 (VII R 43/11) das Screening datenschutzrechtlich für zulässig gehalten. Hiergegen ist einzuwenden, dass die Freiwilligkeit nur im Verhältnis Arbeitgeber – Zollverwaltung vorliegt. Hingegen ist für die Nutzung der Daten des Beschäftigten durch den Arbeitgeber – und zwar ohne wirksames Einverständnis des Beschäftigten – fraglos eine Rechtsgrundlage erforderlich, da es sich um einen einseitigen Eingriff in die Daten des Beschäftigten durch den Arbeitgeber handelt. Im Übrigen verpflichtet eine Rechtsgrundlage, durch die zum Beispiel ein Unternehmen in die Rechte eines Beschäftigten eingreifen darf, grundsätzlich nie zu einem solchen Eingriff, sondern sie erlaubt ihn lediglich. Dies ist das Kernelement einer gestattenden Rechtsgrundlage für ein Handeln zwischen Privatrechtssubjekten. Beispielsweise verpflichtet auch der schon erwähnte § 32 BDSG den Arbeitgeber nicht zu einer Nutzung der Daten des Beschäftigten, sondern erlaubt lediglich eine solche Nutzung. Das zentrale Argument des BFH ist daher nicht nachvollziehbar.

Nur das Unternehmen handelt freiwillig, nicht hingegen der gescreente Arbeitnehmer – damit ist eine Rechtsgrundlage erforderlich.

Bundesgesetzgeber ist gefordert

Es sind somit noch etliche rechtliche Fragen zu klären, um sowohl den Unternehmen als auch den Beschäftigten Rechtssicherheit zu geben. Diese Rechtssicherheit kann nur auf der Grundlage einer hinreichend bestimmten Ermächtigungsgrundlage entstehen. Der Bundesgesetzgeber ist aufgerufen, sie zu schaffen.

Speicherung von Personalausweiskopien: Fast immer rechtswidrig

Regelmäßig erreichen mich Anfragen betroffener Bürger, die sich nach der Rechtmäßigkeit der Anfertigung von Kopien ihres Personalausweises erkundigen. Zwar ist in § 20 Abs. 1 des Personalausweisgesetzes ausdrücklich vorgesehen, dass der Ausweis auch im Wirtschaftsleben als Identitätsnachweis und Legitimationspapier genutzt werden kann. Eindeutige Ausführungen zum Kopieren der Ausweisdaten enthält das Gesetz jedoch nicht.

Nach Auffassung des Bundesinnenministeriums ist das Vervielfältigen von Pässen und Personalausweisen durch Fotokopieren, Scannen oder sonstige Ablichtung aus sicherheitspolitischen und datenschutzrechtlichen Gründen grundsätzlich nicht zulässig. Abgeleitet wird dieses Kopierverbot aus dem Eigentum des Bundes an Pässen und Personalausweisen, der Existenz einiger Erlaubnistatbestände (z. B. im Geldwäschegesetz) sowie indirekt aus § 14 Personalausweisgesetz. Um insbesondere die erheblichen praktischen Schwierigkeiten bei der Identifikation von Betroffenen im Rahmen einer Selbstauskunft nach § 34 Bundesdatenschutzgesetz (BDSG) lösen zu können, lässt das Bundesinnenministerium allerdings die Anfertigung von Ausweiskopien im Einzelfall und unter Beachtung der folgenden strengen Voraussetzungen zu, wenn

Ausweiskopien nur ausnahmsweise und unter strengen Voraussetzungen

- die Erstellung einer Kopie erforderlich ist (dabei muss insbesondere geprüft werden, ob nicht die Vorlage des Personalausweises und gegebenenfalls die Anfertigung eines entsprechenden Vermerks wie z. B. „Personalausweis hat vorgelegen“ ausreicht),
- die Kopie ausschließlich zu Identifikationszwecken verwendet wird,
- die Kopie als solche erkennbar ist,
- nicht für die Identifikation erforderliche Daten, insbesondere die auf dem Ausweis enthaltenen Zugangs- und Seriennummern, geschwärzt werden können und die Betroffenen darauf hingewiesen werden,
- die Kopie unverzüglich vernichtet wird, sobald der damit verfolgte Zweck erreicht ist und
- keine automatisierte Speicherung der Ausweisdaten erfolgt.

Bezogen auf den wirtschaftlich relevanten Auskunfteienbereich haben diese Vorgaben zu folgenden Konkretisierungen geführt:

Im Auskunfteienbereich Vorlage einer Ausweiskopie nur bei nicht eindeutiger Identifizierung

Da das Selbstauskunftsrecht nach § 34 BDSG nur dem Betroffenen zusteht, sind die Auskunfteien gehalten, dessen Identität zur Vermeidung von Personenverwechslungen und Identitätsmissbrauch zu überprüfen. Aber auch in Anbetracht der Tatsache, dass der Betroffene sein Auskunftsrecht in der Regel nicht persönlich, sondern schriftlich geltend macht, ist die Anforderung einer Ausweiskopie auf strittige Einzelfälle einer nicht eindeutigen Identifizierbarkeit zu beschränken. Dies wird bei-

spielsweise dann der Fall sein, wenn zu einem Namen mehrere Anschriften gespeichert sind. Im solchen Einzelfällen haben die Auskunfteien die Betroffenen auch darauf hinzuweisen, dass diese alle über die erforderlichen Identitätsdaten hinausgehenden Angaben auf der Kopie schwärzen können. Für die Identifizierung erforderlich sind grundsätzlich nur Name, Anschrift und Geburtsdatum.

Private Personalausweisdatensammlungen unzulässig

In anderen Wirtschaftsbranchen liegen die Voraussetzungen der Einzelfallregelung zur Anfertigung einer Ausweiskopie dagegen nicht vor. So wurde ich beispielsweise im Rahmen einer Beschwerde auf die Praxis eines großen Logistikdienstleisters in der Automobilbranche hingewiesen, der zur Überwachung des Speditionsvorgangs die Personalausweise der abholenden, nicht zu seinem Betrieb gehörenden Fahrer, einscannt. Die Daten werden anschließend gespeichert und nach Rückmeldung über die Fahrzeugauslieferung an den Kunden gelöscht.
Diese Erhebung und Speicherung personenbezogener Daten bedarf einer Erlaubnisnorm. Die Voraussetzungen der in Betracht kommenden Regelung des § 28 Abs. 1 Satz 1 Nr. 2 BDSG liegen jedoch nicht vor, denn das Vorgehen der Firma ist rechtlich nicht gestattet und zur Wahrung der Unternehmensinteressen auch nicht erforderlich. Weder sind die strengen Voraussetzungen der vom Bundesinnenministerium aufgestellten Ausnahmeregelungen erfüllt noch ist zum Zwecke der Überwachung des Speditionsvorgangs und der Identifizierung des Fahrzeugabholers die Anfertigung von Ausweiskopien erforderlich, wenn – wie hier – der Ausweisinhaber persönlich anwesend ist und den Ausweis vorlegen kann. Es reicht dann aus, dass die Mitarbeiter des Logistikunternehmens über die Vorlage einen entsprechenden Vermerk fertigen und zu Identifizierungszwecken den Namen, die Adresse und gegebenenfalls das Geburtsdatum notieren. Aus ermittlungstaktischen Gründen alle Personalausweisdaten und damit eine private Datensammlung vorhalten zu wollen, ist datenschutzrechtlich nicht zulässig.
Da das Logistikunternehmen nicht bereit war, die rechtswidrige Kopierpraxis zu ändern, habe ich eine entsprechende Untersagungsanordnung nach § 38 Abs. 5 Satz 2 Bundesdatenschutzgesetz mit Androhung eines Zwangsgeldes erlassen. Dagegen hat sich das Unternehmen auf dem Klagewege zur Wehr gesetzt. Das Verwaltungsgerichtsverfahren war im Berichtszeitraum noch nicht abgeschlossen.

Schwerpunktprüfung Callcenter: Starkes Interesse am Schutz der Kundendaten

In meinem letzten Tätigkeitsbericht hatte ich von der Schwerpunktprüfung Callcenter berichtet und dargestellt, mit welchem Konzept und Handlungsschwerpunkten diese Kontrollen durchgeführt wurden. Die Ergebnisse der Prüfungen zeichnen insgesamt ein positives Bild von der Tätigkeit der Callcenter.

Die Vielseitigkeit der Unternehmensform Callcenter und der sehr mannigfaltigen Geschäftsideen lassen keine pauschale Beurteilung zu. Es gibt Betriebe, die mit mehreren hundert Mitarbeitern große Konzerne bei deren Kundenbetreuung unterstützen oder nur als interner Dienstleister innerhalb einer Holding arbeiten. Ferner gibt es kleinere Callcenter, die Einzelaufträge aus der Wirtschaft mit nur wenigen Mitarbeitern erledigen. In den meisten Fällen war der Betrieb eines Callcenters als Auftragsdatenverarbeitung einzuordnen. Damit lag die Verantwortlichkeit für die Datenverarbeitung der Kundendaten beim Auftraggeber. Im Rahmen der Kontrolle wurden auch die verschärften Pflichten des Auftraggebers geprüft und die Umsetzung der neuen Regelungen zu § 11 Bundesdatenschutzgesetz (BDSG) abgefragt.

Die geprüften Unternehmen arbeiteten sehr kooperativ mit mir zusammen. Vorschläge zur Verbesserung sowie Anregungen und Hinweise wurden gern angenommen, und das Bemühen um einen optimalen Datenschutz für die Kundendaten war regelmäßig vorhanden. Ein Zusammenhang zwischen der Größe eines Unternehmens und einem besseren oder schlechteren Datenschutzniveau war nicht zu erkennen. Einige Callcenter hatten sich aufgrund der Anforderungen ihrer Auftraggeber für den Bereich Datenschutz zertifizieren lassen. Andere Unternehmen hatten einen betrieblichen Datenschutzbeauftragten bestellt.

Einige Callcenter hatten sich für den Bereich Datenschutz zertifizieren lassen,andere einen betrieblichen Datenschutzbeauftragten bestellt.

Die von den Unternehmen mitunter sogar über die gesetzliche Norm hinaus bestellten betrieblichen Datenschutzbeauftragten besaßen durchweg die erforderliche Fachkunde und Zuverlässigkeit. Eine Interessenkollision mit anderen betrieblichen Aufgaben konnte ich nicht feststellen. Die nach § 5 BDSG erforderliche Verpflichtung der Beschäftigten und die Schulungen der Mitarbeiter waren durchgeführt worden.

Alle geprüften Callcenter hatten eine strikte Mandantentrennung eingerichtet. Die Mitarbeiter konnten nur auf projektbezogene Daten entsprechend der Funktion und des Berechtigungskonzeptes zugreifen. Die Datenübermittlung zwischen Auftraggebern und Callcenter erfolgte generell verschlüsselt. Die Datenrückgabe an den Auftraggeber bzw. die Löschung der Daten nach Abschluss des Auftrages waren in allen kontrollierten Betrieben geregelt.

Insgesamt ist festzuhalten, dass aufgrund der früheren Skandale und Datenschutzpannen sowie der mehrjährigen Kontrolltätigkeit meiner Behörde die Callcenterbranche ein starkes Eigeninteresse entwickelt hat, die Datenverarbeitung und die Datensicherheit einwandfrei nach den gesetzlichen Bestimmungen des Datenschutzrechts zu gestalten. Dies dient wiederum auch der Vertrauensbildung und Zuverlässigkeit, die in Bezug auf die Auftraggeber unbedingt erforderlich ist.

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.

Der Auskunftsanspruch des § 34 BDSG – und seine Grenzen

§ 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) gewährt einen Auskunftsanspruch über die gespeicherten personenbezogenen Daten. Der Auskunftsanspruch besteht gegenüber der sogenannten verantwortlichen Stelle, also in der Regel der Stelle, bei der die jeweiligen Daten vorliegen. Konkret hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über die zu seiner Person gespeicherten Daten, die Herkunft der Daten, den Empfänger bei Weitergabe der Daten und den Zweck der Speicherung.

Um diesen Auskunftsanspruch ging es bei folgender Petition: Die Petentin verlangte von ihrer privaten Krankenversicherung die Herausgabe eines psychiatrischen Gutachtens, das aus Anlass ihrer Entlassung aus einer psychiatrischen Klinik gefertigt worden war. Als die Versicherung dies ohne nähere Begründung ablehnte, beschwerte sich die Petentin über diese vermeintlich grundlose Weigerung bei meiner Behörde. Die Beschwerde über die Versicherung war jedoch unbegründet, weil das geforderte Gutachten bei der Versicherung nicht (mehr) vorlag. Vielmehr hatte die Klinik das Entlassungsgutachten nur in einem doppelten Umschlag der Versicherung zukommen lassen. Die Versicherung wiederum hatte den inneren Umschlag – weiterhin verschlossen – an ihren fachärztlichen Berater weitergesandt, um von ihm lediglich zu erfahren, ob für den Klinikaufenthalt Versicherungsschutz besteht. Das Gutachten verblieb sodann bei dem fachärztlichen Berater, der als selbständiger Arzt nicht in die Organisationsstruktur der Versicherungsgesellschaft eingebunden war. Meine Prüfung ergab also, dass jedenfalls gegenüber der Versicherung kein Auskunftsanspruch gemäß § 34 Abs. 1 BDSG bestand, da die erwünschte Information zum Zeitpunkt des Auskunftsbegehrens dort nicht vorlag. Der Auskunftsanspruch des § 34 Abs. 1 BDSG erstreckt sich somit nur auf die Daten, die bei der verantwortlichen Stelle vorliegen. Die Versicherung war jedoch nicht verpflichtet, sich im Rahmen eines solchen Auskunftsbegehrens Daten, die bei ihr nicht vorliegen, von dritter Stelle zu beschaffen.

Die Versicherung war nicht verpflichtet, sich im Rahmen eines Auskunftsbegehrens Daten, die bei ihr nicht vorliegen, von dritter Stelle zu beschaffen.

Datensparsamkeit: Nicht jeder darf alles wissen

Diese Trennung ist datenschutzrechtlich sogar geboten. Denn nur auf diese Weise kann eine Trennung zwischen der Leistungsabteilung der Versicherung einerseits und ihrem fachmedizinischen Dienst (hier dem externen fachärztlichen Berater) andererseits erfolgen. Hierin kommt der Grundsatz der Datensparsam-

keit zum Ausdruck, der in § 3a BDSG geregelt ist. Die Leistungsabteilung erhält somit nur diejenigen Daten, die sie (zwingend) benötigt, um zum Beispiel eine Maßnahme zu bewilligen. Hierzu genügt die Information ihres externen fachärztlichen Beraters, ob der Versicherungsschutz die konkrete Maßnahme umfasst, eventuell zusammen mit einer stichpunktartigen Diagnose, sofern dies für die Leistungserbringung erforderlich ist. Die Details eines ärztlichen Gutachtens müssen der Leistungsabteilung dagegen nicht bekannt sein. Der Grundsatz der Datensparsamkeit führt dazu, dass solche „überflüssigen" Daten der Leistungsabteilung auch nicht bekannt sein dürfen.

Ich konnte der Petentin somit nur raten, sich an diejenige verantwortliche Stelle zu wenden, bei der das Gutachten vorliegt, ihren Auskunftsanspruch also in erster Linie bei der Klinik geltend zu machen.

Im Übrigen ist auf Folgendes hinzuweisen: Bezieht sich das Auskunftsbegehren auf besonders sensible medizinische Diagnosen, so dass die Auskunft schwere seelische Erschütterungen hervorrufen kann, so ist anstelle der postalischen Auskunft eine andere Auskunftsform geboten (§ 34 Abs. 6 BDSG). Hierbei wird vor allem eine Mitteilung durch einen Arzt des Vertrauens in Betracht kommen. Darauf kam es in dem oben beschriebenen Fall jedoch nicht mehr an.

Versicherungswirtschaft: Datenschutzverbesserungen durch HIS und Code of Conduct

Nach langjährigen und intensiven Erörterungen zwischen den Datenschutzaufsichtsbehörden und dem Gesamtverband der Deutschen Versicherungswirtschaft (GDV) konnten bei der datenschutzgerechten Ausgestaltung der Datenverarbeitung im Versicherungsbereich erhebliche Verbesserungen erzielt werden.

Hinweis- und Informationssystem (HIS) neu konzipiert

Bei der Prüfung eines Versicherungsantrags oder im Schadensfall kann es zur Verhinderung von Versicherungsmissbrauch notwendig sein, bei anderen Versicherungen Auskünfte einzuholen oder Daten an diese weiterzugeben. Die Versicherungswirtschaft hat deshalb das Hinweis- und Informationssystem (HIS) entwickelt, das der Risikobewertung und Betrugsprävention dient. Betrieben wurde diese Warndatei in der Vergangenheit vom GDV. Bereits 2007 meldeten die Datenschutzaufsichtsbehörden grundsätzliche datenschutzrechtliche Bedenken an, die sich unter anderem auf die mangelnde Transparenz und Kontrollierbarkeit des Datenaustausches zwischen den beteiligten Versicherungen, die Einmeldekriterien sowie die von den Versicherungsunternehmen vorformulierte Einwilligungserklärung bezogen. Sie vereinbarten mit dem GDV eine befristete Weiternutzung des Systems unter der Auflage einer zeitnahen datenschutzgerechten Umgestaltung.
Das neu konzipierte HIS wurde am 1. April 2011 von der Informa Insurance Risk and Fraud Prevention (IIRFP) in Baden-Baden in Betrieb genommen. Es wird als Auskunftei auf der Grundlage des Bundesdatenschutzgesetzes (BDSG) geführt. Daher ist für die Einmeldung der Daten, für die Speicherung und für den Datenabruf durch das Versicherungsunternehmen nicht mehr die Einwilligung des Versicherungsnehmers notwendig. Das Betreiberunternehmen erteilt Auskünfte nur an Versicherungen, vorausgesetzt, diese legen ein berechtigtes Interesse dar. Sofern eine Versicherung eine Einmeldung an das HIS vornimmt, hat sie den Betroffenen unverzüglich zu benachrichtigen. Dieser kann auf diese Weise frühzeitig eine Selbstauskunft über die über ihn gespeicherten Daten beantragen. Gesundheitsdaten werden über das HIS nicht ausgetauscht.

Neue Musterklausel ersetzt Pauschaleinwilligungsklauseln

Im Versicherungsbereich setzt der Umgang mit besonders sensiblen Arten personenbezogener Daten – wie Gesundheitsdaten – die Einholung einer Einwilligung des Betroffenen und die Entbindung seiner behandelnden Ärzte von der

Schweigepflicht voraus. Die dafür von den Versicherungsunternehmen seit Anfang der 1990er-Jahre benutzten Pauschaleinwilligungsklauseln waren insgesamt nicht transparent und entsprachen nicht den Vorschriften des § 4a BDSG. Hierauf bin ich bereits in meinem XVIII. Tätigkeitsbericht (S. 11 ff.) sowie im XIX. Tätigkeitsbericht (S. 26) eingegangen. Entwickelt wurde eine neue, als Bausteinsystem gestaltete Musterklausel für die Einwilligung in die Erhebung und Verwendung von Gesundheitsdaten und Schweigepflichtentbindungserklärungen. Die in vier Abschnitte untergliederte Musterklausel gibt einen maximalen Rahmen für die Einwilligungs- und Schweigepflichtentbindungserklärung vor. Wegen des Prinzips der Datensparsamkeit sind die Versicherungen aber gehalten, nur die Textpassagen zu verwenden, die tatsächlich benötigt werden. Soweit zum Beispiel im Rahmen einer Versicherungssparte oder eines Versicherungsprodukts bestimmte Datenverarbeitungen nicht erfolgen, wie etwa die Erhebung von Gesundheitsdaten bei Dritten zur Risikoprüfung, ist der Text entsprechend zu kürzen.

- Der erste Baustein der Einwilligung betrifft die Erhebung, Speicherung und Nutzung von Gesundheitsdaten durch die Versicherung, die der Antragsteller oder Versicherungsnehmer selbst mitgeteilt hat. Der Mustertext bezieht sich dabei ausdrücklich nur auf solche Daten, die erforderlich sind zur Prüfung eines Versicherungsantrags oder zur Begründung, Durchführung oder Beendigung eines Versicherungsvertrages.
- Der zweite Baustein befasst sich mit der Abfrage von Gesundheitsdaten bei Dritten, wie etwa bei Ärzten oder Angehörigen anderer Heilberufe. Eine solche soll nur stattfinden, soweit sie zur Risikobeurteilung bei einem Versicherungsantrag oder zur Prüfung der Leistungspflicht erforderlich ist. Dabei hat der Antragsteller oder Versicherungsnehmer die Wahl zwischen einer Pauschal- und einer Einzeleinwilligung. Er kann entweder generell in die Datenabfrage bei Dritten zu den in der Klausel festgelegten Zwecken einwilligen oder aber auch erklären, in jedem Einzelfall informiert zu werden und dann zu entscheiden, ob er in die konkrete Abfrage einwilligt oder die erforderlichen Unterlagen selbst beibringt.
- Der dritte Abschnitt regelt die Weitergabe von Gesundheitsdaten durch die Versicherung an andere Stellen außerhalb der Versicherung. In Betracht kommen kann eine Datenweitergabe an medizinische Gutachter, Rückversicherungen oder selbständige Vermittler sowie ein Datenaustausch mit dem HIS.
- Der vierte Abschnitt befasst sich mit dem Umgang mit Gesundheitsdaten bei Nichtzustandekommen des Versicherungsvertrages und der dreijährigen Speicherfrist.

Nachdem die Datenschutzaufsichtsbehörden dieser gemeinsam mit dem GDV entwickelten Musterklausel zugestimmt haben (Beschluss des Düsseldorfer Kreises vom 17.1.2012) sind die Versicherungsunternehmen nunmehr aufgefordert, ihre bisherigen Einwilligungstexte zeitnah durch neue, die den Vorgaben der Musterlösung entsprechen, zu ersetzen.

Code of Conduct konkretisiert Umgang mit personenbezogenen Daten

In einem weiteren Schritt hat der GDV für die Versicherungsbranche verbindliche Verhaltensregeln für den Umgang mit personenbezogenen Daten aufgestellt (Code of Conduct). Damit sind die gemeinsam mit den Datenschutzaufsichtsbehörden vorangetriebenen Arbeiten an der Entwicklung von datenschutzgerechten Verhaltensregelungen, auf die ich bereits in meinem XIX. Tätigkeitsbericht (S. 26) eingegangen bin, nunmehr abgeschlossen. Nach Unterbreitung des Entwurfs der Verhaltensregelungen hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit mit Feststellungsbescheid vom 2.11.2012 deren Vereinbarkeit mit dem geltenden Datenschutzrecht erklärt und sie als bereichsspezifische Verhaltensregelung im Sinne des § 38a BDSG anerkannt.
Beabsichtigt ist mit dem Code of Conduct, die Regelungen des Bundesdatenschutzgesetzes für die Versicherungsbranche zu konkretisieren und zu ergänzen und weitestgehend einheitliche Standards zu schaffen. Als Spezialregelungen erfassen sie die wichtigsten Verarbeitungen personenbezogener Daten, welche die Versicherungsunternehmen im Zusammenhang mit der Begründung, Durchführung, Beendigung oder Akquise von Versicherungsverträgen vornehmen. Mit den Verhaltensregeln sollen zusätzliche Einwilligungen entbehrlich gemacht werden. Erforderlich sein sollen diese grundsätzlich nur noch für die Verarbeitung von besonders sensiblen Arten personenbezogener Daten – wie Gesundheitsdaten – sowie für die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung.

Auskunfteien: Das vielschichtige Geschäft mit Bonitätsbewertungen und Scores

Auskunfteien dürfen aufgrund der gesetzlichen Vorgaben in den §§ 28b Nr. 2, 29 Bundesdatenschutzgesetz (BDSG) für die Berechnung eines Scorewertes grundsätzlich alle dafür erforderlichen und geeigneten personenbezogenen Daten über einen Betroffenen erheben und die zu ihm bereits gespeicherten Daten, die den Anforderungen des § 28a Abs. 1 und 2 BDSG genügen, nutzen, soweit diese Daten einen Zusammenhang mit dessen Bonität aufweisen. Bei einem aus solchen rechtmäßig erhobenen Daten berechneten so genannten Scorewert handelt es sich allerdings auch dann um ein subjektives Werturteil der jeweiligen Auskunftei, wenn der Score mittels eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens im Sinne des § 28b Nr. 1 BDSG gebildet wurde. Daher muss jedes Bonitätsurteil, auch wenn es als mathematisch-statistisch ermittelter Scorewert daherkommt, auf zutreffenden und sachlich gehaltenen Informationen beruhen. Denn solche Werturteile, die schließlich nur zum Zweck der Auskunft an Dritte gebildet werden, sind personenbezogene Daten im Sinne des BDSG.

Im Berichtszeitraum hatte ich Anlass, auf der Grundlage dieser Maßstäbe das Verfahren einer niedersächsischen Auskunftei zur Bonitätsbildung einer kritischen Prüfung zu unterziehen. Ausgangspunkt war die Eingabe einer Einzelperson, die sich darüber beschwert hatte, das zu ihr von dieser Auskunftei gebildete und Dritten mitgeteilte Bonitätsurteil sei zu schlecht, es beruhe auf unzureichenden bonitätsrelevanten Daten und sei kreditgefährdend.

Bonitätsaussagen und Scores sind immer Werturteile über die Kreditwürdigkeit des Betroffenen (BGH, Urteil vom 22.2.2011 -VI ZR 120/10-)

Die datenschutzrechtliche Untersuchung dieses Einzelfalles ließ auf den ersten Blick tatsächliche Zweifel daran aufkommen, dass die Auskunftei, die auch als Inkassounternehmen tätig ist, ein sachlich zutreffendes Bonitätsurteil abgegeben hatte. Denn Bonitätsbewertungen sind als datenschutzrelevante Werturteile insbesondere dann zu beanstanden, wenn (so auch Krämer, NJW 2012, S. 3201 ff. m. w. N.)

- sie auf einer nicht ausreichenden Anzahl von Faktoren basieren,
- unzureichende oder unzulässige Faktoren in die Berechnung einbezogen worden sind oder
- sie auf einer Fehlgewichtung einzelner Faktoren beruhen.

Nicht bonitätsrelevante und daher unzulässige Faktoren sind dabei

- unverbindliche Kreditkonditionenanfragen bei einer Bank,
- Angaben zum Kauf- und Verbraucherverhalten des Betroffenen,
- die Anzahl der bei einer Auskunftei zu einer Person eingegangenen Bonitätsanfragen,
- abgebrochene Vertragsverhandlungen sowie
- Angaben zu Wohndauer, Nationalität, Bildungsabschlüssen, Geschlecht und Familienstand.

Nur bonitätsrelevante Daten dürfen zugrunde gelegt werden

Die Prüfung hatte hier ergeben, dass das vom Petenten kritisierte Bonitätsurteil auf nur einer offenen Forderung als einem sachlichen Bonitätsnegativmerkmal beruhte. Die Forderung stammte zudem aus dem Datenbestand der daneben betriebenen Inkassoabteilung der Auskunftei. Solche Einmeldungen offener Inkassoforderungen in den Datenbestand der eigenen Auskunftei sind zwar gemäß § 28a Abs. 1 S. 2 BDSG zulässig, wenn die übrigen Einmeldevoraussetzungen des § 28a Abs. 1 BDSG vorliegen. Das ist unter anderem der Fall, wenn – wie im vorliegenden Fall – die unbestrittene Forderung fällig ist und nach Maßgabe des § 28a Abs. 1 Nr. 4 BDSG erfolglos gemahnt worden war.

Bonitätsbewertung nur bei ausreichender Datenbasis

Hier war aber der Frage nachzugehen, welchen Charakter die aus diesem einzigen negativen Einmeldedatum gebildete schlechte Bonitätsbewertung hatte. Nach Auffassung der geprüften Auskunftei stellte die Negativbewertung jedenfalls keinen Score im Sinne des § 28b BDSG dar, da auch nach den Vorstellungen der Auskunftei die Voraussetzungen eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens bei der Bildung des Bonitätswerts nicht erfüllt waren. Die Bonitätsaussage zu dem Petenten war vielmehr nur das Ergebnis einer groben dreistufigen und in den Ampelfarben visualisierten Bewertung (hier: rot). Mit der sich hieraus ergebenden weiteren Frage, ob es seit dem Inkrafttreten der Scoringvorschrift am 1.4.2010 im Bereich der Auskunfteien Bonitätsbewertungen auch außerhalb des § 28b BDSG geben kann, habe ich auch die AG Auskunfteien, eine Arbeitsgruppe des Düsseldorfer Kreises, befasst. Ergebnis: Das von der geprüften Auskunftei praktizierte Bonitätsbewertungsverfahren mittels Ampeldarstellung ist nur dann außerhalb des Scoringverfahrens i. S. d. § 28b BDSG zulässig, wenn neben der durch Text, Zahl und/oder Ampelvisualisierung erfolgenden summarischen Bonitätsaussage zusätzlich auch die der Bewertung zugrunde liegenden Daten mitgeteilt werden. Dies bedeutet im Umkehrschluss, dass die Übermittlung unzulässig wird, sobald nur eine summarische Bonitätsaussage – gleich welcher Form – getroffen und weitergegeben wird. Denn eine Auskunftei darf nur entweder konkrete und belegte Daten übermitteln oder einen Score, der den Anforderungen des § 28b BDSG genügt.

Beauskunftung einer lediglich summarischen Bonitätsaussage nur zusammen mit den Daten, die der Bewertung zugrunde liegen

Da die Prüfung ergab, dass die Auskunftei neben ihrem „Ampel"-Werturteil auch die zugrunde liegenden Daten übermittelt hatte, blieb die Bewertungspraxis unbeanstandet. Dennoch gab die Bewertung des Petenten im konkreten Fall Anlass zu datenschutzrechtlicher Beanstandung: Bei dessen negativer Bonitätsbewertung durch die Auskunftei handelte es sich um ein subjektives Werturteil, das nur dann hätte gebildet und als perso-

nenbezogenes Datum beauskunftet werden dürfen, wenn es unter anderem auf einer ausreichenden Anzahl von zutreffenden und zulässigen Bewertungsfaktoren basiert hätte. Diese Voraussetzung war jedoch nicht erfüllt. Denn das Vorliegen nur eines Inkassofalles genügt den Anforderungen an eine ausreichende Datenbasis nicht. Die Beauskunftung dieser Bonitätsbewertung war daher rechtswidrig.

Berechtigtes Interesse an der Auskunft muss stichprobenartig geprüft werden

Daneben brachte die breit angelegte und alle Arbeitsabläufe sowie die technisch-organisatorischen Maßnahmen umfassende Prüfung auch zutage, dass die Auskunftei ihre aus § 29 Abs. 2 S. 5 BDSG folgende Obliegenheit, zeitnah und mit einem geeigneten Stichprobenverfahren zu prüfen, ob das von den Auskunftsempfängern glaubhaft gemachte berechtigte Interesse an der Beauskunftung tatsächlich vorlag, grob vernachlässigt hatte. Nachdem ich die Auskunftei von der datenschutzrechtlichen Relevanz eines effektiven Stichprobenkonzepts überzeugen konnte, gab sie ihre bisherige rudimentäre und den gesetzlichen Anforderungen nicht gerecht werdende Stichprobenpraxis auf und verfährt nunmehr datenschutzkonform:

- Information an den Kunden als Bestandteil der AGB bereits vor Auskunfterteilung über die Anforderungen an ein ordnungsgemäßes Stichprobenverfahren, damit er über den Zweck der Stichproben, seine Angaben zum berechtigten Beauskunftungsinteresse zu verifizieren, und seine Mitwirkungspflicht informiert ist,
- Dokumentation
  - der Zeitabschnitte, für die Stichproben erfolgen,
  - der Stichprobenbildung auf der Grundlage von zwei Promille des Anfrageaufkommens im jeweiligen Stichprobenzeitraum,
- Prüfung eingegangener Rückantworten auf Vollständigkeit und bezüglich der Frage, ob eine durch beigefügte Unterlagen belegte Kongruenz besteht zwischen dem ursprünglich angegebenen und dem im Stichprobenverfahren genannten Abfragegrund,
- Nachfragen bei fehlender, unvollständiger oder nicht plausibler Antwort,
- Sanktionen im Fall fehlender oder nicht ordnungsgemäßer Antworten, und zwar
  - Abmahnungen gegenüber den Kunden mit der Androhung des künftigen Ausschlusses vom Auskunftsbezug sowie Androhung der Anzeige wegen eines bußgeldbewehrten Datenschutzverstoßes bei der Datenschutzaufsichtsbehörde,
  - Ausschluss vom Auskunftsbezug,
  - Anzeige bei der Aufsichtsbehörde.

Bei Kontrollen werde ich künftig insbesondere prüfen, ob niedersächsische Auskunfteien nach dem vorgestellten oder einem gleichwertigen Stichprobenkonzept vorgehen.

Vermieter informieren Vermieter: Geschäftsmodell gescheitert, Daten gelöscht

Vermieter sind bestrebt, so viele Informationen wie möglich über einen Mietinteressenten zu erlangen, um letztlich Klarheit über die Bonität des künftigen Mieters zu gewinnen. Gewerbliche Vermieter und Wohnungsbaugenossenschaften werden deshalb in erster Linie auf entsprechende Informationen von Wirtschaftsauskunfteien zurückgreifen, was grundsätzlich nicht zu beanstanden ist, wenn die datenschutzrechtlichen Voraussetzungen solcher Auskunfteianfragen beachtet werden (siehe auch meinen XX. Tätigkeitsbericht, S. 47). Privaten Vermietern ist der Zugang zu Wirtschaftsauskunfteien jedoch häufig verwehrt, so dass sie auf andere Quellen angewiesen sind, um sich über die Bonität eines Mietinteressenten zu informieren.

Diesen Informationsbedarf versuchen seit einiger Zeit Online-Mieterbewertungsportale zu decken, indem sie unter dem Motto „Vermieter informiert Vermieter“ die Möglichkeit bieten, Bewertungen des Verhaltens der Mieter und Erfahrungen mit ihnen in das Portal einzustellen, um anderen Vermietern den Abruf dieser Bewertungen zu ermöglichen. Damit erhalten potentielle neue Vermieter unter anderem bonitätsrelevante Informationen über Mietinteressenten. Auf ein solches in Niedersachsen ansässiges Portal bin ich aufgrund seiner Anmeldung zum Register nach § 38 Abs. 2 Bundesdatenschutzgesetz (BDSG) und einer Reihe von Beschwerden Betroffener aufmerksam geworden und habe das Geschäftsmodell datenschutzrechtlich überprüft. Dem einmeldenden Vermieter bot das Portal im Wesentlichen die Möglichkeit, zu konkret benannten Mietern die folgenden miet- und bonitätsrelevanten Informationen mitzuteilen:

- Zahlungsmoral des Mieters,
- Bewertung der Wohnungsübergabe bei Mietende,
- Einhaltung der Hausordnung,
- Pflegezustand der Wohnung,
- termingerechte Überweisung einer Kaution,
- Verhalten des Mieters innerhalb der Mietergemeinschaft und
- vereinbarungsgemäße Nutzung der Wohnung.

Erforderliche Erklärung des Vermieters wurde nicht überprüft.

Um diese Daten abrufen zu können, musste sich der an ihnen interessierte potentielle Vermieter im Online-Portal anmelden und verbindlich erklären, dass er ein berechtigtes Interesse im Sinne des § 29 Abs. 2 S. 1 Nr. 1 BDSG an der Kenntnis der Mieterinformationen habe. Eine Überprüfung dieser Erklärung durch den Anbieter des Portals erfolgte allerdings ebenso wenig wie eine Stichprobenprüfung nach Maßgabe des § 29 Abs. 2 S. 5 BDSG.

Subjektive Einschätzungen, wenig Aussagegehalt

Aufgrund dieser Ausgestaltung der Portalnutzung war schnell klar, dass hier eine Mieter-Auskunftei betrieben wurde, die datenschutzrechtlich nach § 29 BDSG zu beurteilen war.

Bereits die datenschutzrechtliche Zulässigkeit der Erhebung und Speicherung der von Vermietern eingemeldeten Informationen und Bewertungen war allerdings zu verneinen. Denn der alleine als Erhebungsgrundlage in Betracht kommende § 29 Abs. 1 Nr. 1 BDSG scheiterte hier an entgegenstehenden schutzwürdigen Interessen der von der Datenerhebung betroffenen Mieter. Zum einen waren die Vermieterbewertungen zu den oben genannten Bewertungssachverhalten in hohem Maße von subjektiven Einschätzungen geprägt, kaum objektivierbar und wiesen daher einen nur geringen bonitätsrelevanten Aussagegehalt auf. Zum anderen war zu berücksichtigen, dass die Wohnung eine große Bedeutung für die Lebensgestaltung hat und deshalb das Interesse der Mietinteressenten, den Erfolg ihrer Wohnungssuche nicht von der Bewertung des ehemaligen Vermieters abhängig zu machen, Vorrang hatte vor kaum belastbaren Informationen der Vermietereinschätzungen zum Mieterverhalten.

Aus denselben Gründen war im Übrigen aber auch eine Übermittlung der Vermieterinformationen und -bewertungen an interessierte andere Vermieter über das Online-Portal unzulässig. Denn nach § 29 Abs. 2 S. 1 Nr. 2 BDSG dürfen personenbezogene Daten nur dann an berechtigte Dritte übermittelt werden, wenn kein Grund zu der Annahme besteht, dass der betroffene Mieter ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat.

Online-Portale, in denen Vermieter Erfahrungen mit Mietern ohne deren Einwilligung weitergeben, sind unseriös und unzulässig.

Mit anderen Worten: Der Betreiber dieser Mieter-Auskunftei hätte sein Geschäftsmodell nur dann fortsetzen können, wenn die Einmeldungen seitens der Vermieter aufgrund einer wirksamen Einwilligung der Mieter gem. § 4a BDSG erfolgt wären. Da solche Einwilligungen nicht vorlagen und der Betreiber des Online-Portals seiner einmeldenden Kundschaft die Vorlage von Einwilligungen ihrer Mieter nicht zumuten wollte, war das Geschäftsmodell gescheitert, und die zu Unrecht erhobenen Daten mussten gelöscht werden.

Anmeldung zum VHS-Kurs: Kontodatenübermittlung per Postkarte

Ein Petent wandte sich an mich, nachdem er im Fernsehen eine Sendung zum Problem „sensible Daten im Papiermüll" gesehen hatte, in welcher der datenschutzgerechte Umgang mit persönlichen Daten wie zum Beispiel Konto- und Krankheitsdaten thematisiert wurde.

Kurz darauf erhielt er von seiner örtlichen Volkshochschule (VHS) das neue Programm, dem Anmeldekarten zu den dort angebotenen Kursen beilagen. Auf dieser Karte sollten die Teilnehmer nicht nur die gewünschten Kurse eintragen, sondern zudem – neben den Kontaktdaten – auch die Kontodaten. Die Kursgebühren würden im Lastschriftverfahren erhoben, andernfalls, bei Rechnungsstellung, fiele eine zusätzliche Gebühr von drei Euro an.
Die Auffassung des Petenten, dass die Übermittlung der besonders zu schützenden Kontodaten nicht über das jedermann leicht zugängliche Medium Postkarte erfolgen sollte, teilte ich. Daher nahm ich Kontakt zum Datenschutzbeauftragten des Trägers der Einrichtung auf und bat diesen zu veranlassen, dass die VHS das Adressfeld ihrer Anmeldekarten mit dem Hinweistext „Bitte in einem verschlossenen Umschlag zurücksenden" versehen wird. Darüber hinaus sollte auf den Text „Postkarte" sowie „Bitte ausreichend frankieren" verzichtet werden.
Die von mir vorgeschlagene datenschutzkonforme Überarbeitung wird mit dem neuen Programmheft umgesetzt.

Sozialverbände: Mitgliederdaten an Versicherungen weitergegeben

Ein Mitglied eines Sozialverbands wandte sich an mich, da es von einer Versicherung eine Postkarte mit der Ankündigung des Hausbesuchs durch einen Versicherungsvertreter erhalten hatte. Auf dieser Karte war auf die Mitgliedschaft im Sozialverband hingewiesen worden. Aus der Presse erfuhr ich von einem ähnlich gelagerten Fall eines weiteren Sozialverbandes, weshalb ich beide Verbände voneinander unanhängig zu einem Gespräch in meine Dienststelle einlud.

Sozialverbände sind Interessenverbände, die die politischen und sozialen Interessen von Rentnern, Arbeitslosen, Sozialhilfeempfängern, Versicherten der gesetzlichen Krankenversicherung, Behinderten, Unfallopfern, Pflegefällen oder von Handwerkern vertreten. Die Übermittlung der personenbezogenen Daten erfolgte in beiden Fällen im Rahmen von sogenannten Gruppenversicherungsverträgen. Hierbei handelt es sich um Rahmenverträge zwischen Vereinen oder Verbänden und Versicherungsunternehmen, die den Mitgliedern unter bestimmten Voraussetzungen den Abschluss von Einzelversicherungsverträgen zu günstigeren als den üblichen Konditionen ermöglichen. Zwar erlaubt § 28 Abs. 3 Bundesdatenschutzgesetz (BDSG) in Satz 4 die listenmäßige Übermittlung personenbezogener Daten zu Werbezwecken, schränkt dieses im folgenden Satz 6 jedoch dahingehend wieder ein, dass eine solche Verarbeitung nur zulässig ist, soweit schutzwürdige Interessen der Betroffenen nicht entgegenstehen.

Schutzwürdige Interessen verbieten Datenübermittlung

Gerade bei den Mitgliedern eines Sozialverbandes stehen die schutzwürdigen Interessen regelmäßig einer Übermittlung ihrer Adressdaten an Dritte entgegen. Die hier betroffenen Mitgliederdaten stehen im Kontext mit Gesundheitsdaten und damit mit besonderen Arten personenbezogener Daten (§ 3 Abs. 9 BDSG). Vor diesem Hintergrund hat der Düsseldorfer Kreis, der Zusammenschluss der obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, bereits in seiner Sitzung am 24./25.11.2010 zum Thema Gruppenversicherungsverträge einen Beschluss gefasst, wonach die Übermittlung personenbezogener Daten von Vereinsmitgliedern an ein Versicherungsunternehmen für die Werbung zum Abschluss solcher Verträge die freiwillige und informierte Einwilligung (§ 4a Abs. 1 BDSG) der Betroffenen voraussetzt. In Bezug auf Altmitglieder wurde bisher eine Information mittels Avisschreibens mit der Möglichkeit des Widerspruchs für ausreichend ge-

halten. Die Aufsichtsbehörden haben in ihrem Beschluss aber festgestellt, dass auch für Altmitglieder die vorherige Einholung einer informierten Einwilligungserklärung nunmehr erforderlich ist.

Schriftliche Einwilligung erforderlich

Um diesen datenschutzrechtlichen Anforderungen zu entsprechen, wurden die beiden Sozialverbände gebeten, bei erstmaliger Übermittlung von Adressdaten im Rahmen der Gruppenversicherungsverträge den Beschluss des Düsseldorfer Kreises künftig zu beachten und auch vor der Übermittlung von Adressänderungen das Mitglied im Einzelfall schriftlich zu befragen, ob es mit der Weitergabe seiner geänderten Daten an eine Versicherung einverstanden ist. Die Vertreter beider Verbände sagten diese Vorgehensweise zu. Darüber hinaus empfahl ich eine Veröffentlichung zu dieser Thematik in den jeweiligen Vereinspublikationen (z. B. Mitgliederzeitungen). Zudem regte ich an, die Rechtsauffassung der Aufsichtsbehörden auch auf der jeweiligen Bundesverbandsebene zu thematisieren und für eine datenschutzkonforme Umsetzung einzutreten. Außerdem gab ich meiner Erwartung Ausdruck, dass die Sozialverbände auch durch technisch-organisatorische Maßnahmen sicherstellen, Adressdaten (auch von Altmitgliedern) und deren Aktualisierungen nur noch dann an Dritte zu übermitteln, wenn hierzu Einwilligungen vorliegen und dokumentiert sind.

Weitere Informationen:

Der Beschluss des Düsseldorfer Kreises ist abrufbar unter:
www.lfd.niedersachsen.de >Themen >Vereine

Werbung per Telefon und E-Mail: Sehr oft fehlt die Einwilligung für Datennutzung

Bereits in meinem letzten Tätigkeitsbericht habe ich mich mit verschiedenen datenschutzrechtlichen Aspekten der Werbung und des Adresshandels befasst (XX. Tätigkeitsbericht 2009–2010, S. 44, 53). Auch im aktuellen Berichtszeitraum hat dieser Themenkreis wieder eine große und – unter Datenschutzgesichtspunkten – leider wenig erfreuliche Rolle gespielt.
Dabei ist unbestritten, dass die gezielte werbliche Ansprache des potentiellen Kunden ihre Berechtigung in der Konsumwelt hat und vom Adressaten häufig auch nicht als Belästigung empfunden wird, sondern als willkommene Produktinformation. Wird Werbung aber zum Ärgernis, weil sie unerwünscht ist oder als Störung aufgefasst wird, so stellt der Betroffene schnell die typische und datenschutzrelevante Frage nach der Herkunft seiner Adresse.

Solche regelmäßig wiederkehrenden Fragen sind verständlich: Die gesetzlichen Bestimmungen des Bundesdatenschutzgesetztes (BDSG) und anderer für die Werbewirtschaft bedeutsamer Bestimmungen sind für die Betroffenen und vor allem für juristische Laien nicht leicht zugänglich und teilweise sogar überraschend. So trifft das so genannte Listenprivileg des § 28 Abs. 3 S. 2 BDSG, das eine werbliche Ansprache zum Beispiel von Bestandskunden auch ohne Einwilligung des Adressaten ermöglicht, bei vielen Bürgern immer wieder auf Unverständnis. Ich halte daher auf meiner Internetseite ein „Informationsblatt Adresshandel" zum Download bereit, in dem ausführlich zu wichtigen Fragen im Zusammenhang mit Adresshandel und (unerwünschter) Werbung Auskunft gegeben und die aktuelle Rechtslage erläutert wird. Außerdem findet der Leser dort Tipps zum Beispiel zum Werbewiderspruch und seinen Auskunftsrechten gegenüber den werbenden Unternehmen.

Schwerpunkte sind inzwischen Telefon- und E-Mail-Werbung

Haben bis vor wenigen Jahren datenschutzrechtliche Fragen zur Werbung per Post noch eine große Rolle gespielt, so ist deren Bedeutung mittlerweile deutlich zurückgegangen. Dies mag daran liegen, dass die mit der im Jahr 2009 in Kraft getretenen Neufassung des § 28 Abs. 3 BDSG komplexer gewordenen Datenschutzregelungen zu Werbung und Adresshandel viele unseriöse oder unprofessionell arbeitende Unternehmen dazu veranlasst haben, auf die schnelleren und vermeintlich besser zu handhabenden Werbemedien E-Mail und Telefon auszuweichen. Tatsächlich ist der Trend erkennbar, dass sich die Datenschutzprobleme mittlerweile auf die genannten Medien konzentrieren. Die Rechtslage ist hier seit der Novelle aus dem Jahr 2009 zum Gesetz gegen den unlauteren Wettbewerb (UWG) allerdings ganz eindeutig:

- Werbeanrufe oder Fax-Werbung gegenüber Verbrauchern sind nur noch mit deren vorheriger ausdrücklicher Einwilligung erlaubt. Außerdem dürfen Anrufer bei Werbeanrufen ihre Rufnummer nicht mehr unterdrücken, um ihre Identität zu verschleiern. Verstöße gegen diese UWG-Vorschriften ahndet die Bundesnetzagentur, die hierzu die Beschwerdeseite „Rufnummernmissbrauch" eingerichtet hat.

Die Bundesnetzagentur (www.bundesnetzagentur.de) geht gegen unerwünschte Telefonwerbung vor

- Auch E-Mail-Werbung kann wettbewerbsrechtlich nur dann ohne Einwilligung erfolgen, wenn das werbende Unternehmen im Zusammenhang mit dem Verkauf von Waren oder Dienstleistungen die E-Mail-Adresse von einem Kunden erhalten hat, diese Adresse für die Bewerbung ähnlicher Waren oder Dienstleistungen nutzt und der Kunde der werblichen Verwendung seiner E-Mail-Adresse nicht widersprochen hat. Ist eine dieser Voraussetzungen nicht erfüllt, darf Werbung auch per E-Mail nur mit einer vorherigen ausdrücklichen Einwilligung erfolgen. Sonst liegt eine wettbewerbswidrige so genannte Spam-Mail vor.

Mit den beiden wettbewerbsrechtlich klar geregelten aktuellen Erscheinungsformen von (unerwünschter) Werbung hatte ich mich im Berichtszeitraum auch unter Datenschutzgesichtspunkten verstärkt zu befassen. Denn die Regelungen des UWG zur grundsätzlichen ausdrücklichen Einwilligung von werblicher Ansprache mit diesen Medien hat auch Auswirkungen auf die werberechtlichen Regelungen des § 28 Abs. 3 BDSG: Liegt eine nach UWG erforderliche Einwilligung nicht vor, so ist regelmäßig von entgegenstehenden schutzwürdigen Interessen i. S. d. § 28 Abs. 3 S. 6 BDSG des Betroffenen mit der Folge auszugehen, dass die Werbetreibenden auch nicht auf die Erlaubnisvorschriften des § 28 Abs. 3 S. 2–5 BDSG zur Rechtfertigung ihrer einwilligungslosen Werbung zurückgreifen können. Die werbliche Verwendung der personenbezogenen Daten „Telefonnummer" und „E-Mail-Adresse" ist dann auch datenschutzrechtlich unzulässig und zu unterbinden.

Unrechtmäßige Datensammelei mit Online-Gewinnspielen

So haben Empfänger solcher unerwünschter Telefon- oder E-Mail-Werbung mir gegenüber Klage darüber geführt, die Unternehmen hätten auf Nachfrage die unwahre Behauptung aufgestellt, es liege eine Einwilligung in diese Form der Werbung vor. Die Einwilligung sei im Rahmen eines Online-Gewinnspiels erteilt worden, das von einem dritten Unternehmen veranstaltet worden sei. Dieses Unternehmen habe die Daten für die werbliche Ansprache zur Verfügung gestellt (meist im Rahmen des so genannten Lettershop-Verfahrens vermietet) und dabei die Werbeeinwilligung im „Double-Opt-In-Verfahren" zugesichert.
Die Überprüfung einer Reihe von gleichartigen Sachverhalten bei niedersächsischen Online-Gewinnspielanbietern hat jedoch ergeben, dass das Verfahren zur Generierung von Telefon- oder E-Mail-Adressdaten für Zwecke der Werbung mittels Internet-Gewinnspielen nicht geeignet war, um den Nachweis führen zu können, dass

die (angeblichen) Gewinnspielteilnehmer ihre Einwilligung in die werbliche Nutzung ihrer Daten erteilt haben.

So deckte ich in mehreren Fällen auf, dass das von der Rechtsprechung des BGH (vgl. insbes. Urteil vom 10.2.2011, Az.: I ZR 164/09) als Nachweis verlangte „Double-Opt-In-Verfahren nicht eingehalten worden war. In allen untersuchten Fällen lag dem Gewinnspielanbieter nämlich nicht eine die Einwilligung zweifelsfrei bestätigende Antwort-E-Mail des Gewinnspielteilnehmers vor, sondern nur eine nach der BGH-Rechtsprechung nicht ausreichende IP-Adresse mit digitalem Zeitstempel („timestamp"), die dem Gewinnspielteilnehmer gerade nicht eindeutig zugeordnet werden konnte. In mehreren Fällen konnte zudem ermittelt werden, dass die angeblichen Gewinnspielteilnehmer zu dem vom Gewinnspielanbieter genannten Zeitpunkt ihren Rechner nicht genutzt hatten und daher auch am Online-Gewinnspiel gar nicht teilgenommen haben konnten. Insgesamt entstand in den untersuchten Fällen der Verdacht, dass die Betreiber der online-Gewinnspielseiten die Durchführung eines „Double-Opt-In-Verfahrens" nur vorgetäuscht hatten und zu den für Werbezwecke weitergegebenen Daten in Wahrheit keine Einwilligung mittels Telefon oder E-Mail vorlag.

In einem Fall ist mir darüber hinaus der konkrete Nachweis gelungen, dass die Online-Gewinnspielseiten nur zum Schein vorgehalten wurden, um ein „Double-Opt-In" vorzutäuschen und die auf anderem Weg generierten (zum Beispiel aus Telefonbüchern, Internetseiten) Telefon- oder E-Mail-Daten besser, nämlich mit dem Anschein einer bestehenden Werbeeinwilligung, vermarkten zu können. Ein Fall mit eindeutig strafrechtlicher Relevanz.

Kein wirksames Double-Opt-In, sofern keine Bestätigungs-E-Mail, sondern nur eine IP-Adresse vorliegt.

Alle geprüften niedersächsischen Betreiber von Internet-Gewinnspielen haben nicht zuletzt aufgrund meines entsprechenden aufsichtsbehördlichen Drucks ihr Geschäftsmodell mittlerweile eingestellt und ihre Gewinnspielseiten aus dem Netz entfernt. In einem Fall konnte einem Gewinnspielbetreiber daneben nachgewiesen werden, dass er einem Betroffenen die falsche Auskunft erteilt hat, seine Daten stammten aus dem Gewinnspiel. Diese Falschbeauskunftung habe ich nach Maßgabe des § 43 Abs. 1 Nr. 8a BDSG mit einem Bußgeld geahndet.

Werbende Unternehmen selbst Opfer ihrer Datenlieferanten

Aber auch Nutzer solcher Adressdaten fallen bisweilen auf die falschen Versprechungen ihrer Datenlieferanten herein. So bestätigte mir ein Dienstleister, der die von einem Betreiber einer Gewinnspielseite generierten E-Mail-Adressen für eine werbliche Direktmailingaktion nutzte, dass er außergewöhnlich viele Werbewidersprüche von den Angesprochenen erhalten und erst daraufhin festgestellt habe, dass sein Datenlieferant das zugesicherte „Double-Opt-In" gar nicht nachweisen konnte. Trotz dieses vertragswidrigen Verhaltens des Lieferanten gilt aber auch hier die datenschutzrechtliche Verantwortlichkeit des Verwenders von Daten, von denen er in gutem Glauben angenommen hat, es lägen dazu die erforderlichen Einwilli-

Dem Datennutzer obliegt die Pflicht, die vom Datenlieferanten behauptete Einwilligung in Nutzung für Werbezwecke zu prüfen

gungen in die Nutzung für werbliche Zwecke vor. Der Verwender darf also nicht auf das Versprechen seines Lieferanten vertrauen. Vielmehr muss er im Rahmen von Stichproben vor der Verwendung der zugelieferten Adressdaten die zugesicherte Eigenschaft „Double-Opt-In liegt vor" selbst prüfen, will er nicht selbst in den Fokus einer datenschutzrechtlichen Prüfung geraten. Im konkreten Fall hatte der Dienstleister diese Obliegenheiten nicht beachtet, was ihm im Hinblick auf den ohnehin eingetretenen materiellen und Imageschaden allerdings nur eine Beanstandung meiner Behörde eintrug.

Weitere Informationen:

Informationsblatt zu Werbung und Adresshandel unter
www.lfd.niedersachsen.de >Themen >Wirtschaft >Adresshandel

Einzelhandel will mehr Videoüberwachung

Der Handelsverband Deutschland (HDE), die Spitzenorganisation des deutschen Einzelhandels für rund 400.000 selbständige Unternehmen, bat um eine Besprechung mit den Datenschutzaufsichtsbehörden vor dem Hintergrund der Überlegungen und Planungen zahlreicher Mitgliedsunternehmen (insbesondere Einzelhandelsbetriebe und Einkaufszentren), künftig verstärkt Anlagen zur Videoüberwachung einzusetzen. Dies sei nach Aussage des HDE insbesondere aus Gründen der Arbeitssicherheit und des Arbeitsschutzes geboten. Die Verbands- und Firmenvertreter stellten vor allem auf Raubüberfälle ab, wobei hier Lebensmittelgeschäfte überproportional betroffen seien. Vorrangig ereigneten sich diese Straftaten zu Beginn und gegen Ende der Öffnungszeiten.

Ich wies wie alle übrigen Vertreter der Datenschutzaufsichtsbehörden darauf hin, dass das Datenschutzrecht vom Verbot mit Erlaubnisvorbehalt geprägt sei. Die Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume durch nicht-öffentliche Stellen setze nach § 6b Abs. 1 BDSG u. a. voraus, dass diese zur Wahrnehmung entweder des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich sei. Eine anlasslose flächendeckende Videoüberwachung ohne konkret festgelegten Zweck entspreche nicht dem Willen des Gesetzgebers.

Abschreckende Wirkung nicht nachgewiesen

Die seitens des Verbandes in der Diskussion vorgetragenen präventiven Effekte einer offenen Videoüberwachung wurden von den Vertretern der Datenschutzbeauftragten unter Hinweis darauf, dass eine abschreckende Wirkung empirisch nicht nachgewiesen sei, in Zweifel gezogen. Spezialpräventive Überlegungen, die auf eine Abschreckung von in der Vergangenheit durch einschlägige Straftaten in Erscheinung getretene Personen abzielten, rechtfertigten keinesfalls eine Videoüberwachung, die notwendigerweise eine Vielzahl anderer Personen erfasse. Polizeiliche Erfahrungen auf der Reeperbahn in Hamburg legten zudem den Schluss nahe, dass eine präventive Wirkung der Videoüberwachung nur durch ein Monitoring mit unmittelbarer Krisenintervention erzielt werden könne. Es stelle sich die Frage, ob gerade durch eine Videoüberwachung im Einzelhandel die erhofften Effekte erreichbar seien. In manchen Fällen ließen sich anderweitige Kontrollmaßnahmen (etwa bei der Warenrücknahme) umsetzen, die eine Videoüberwachung ersichtlich entbehrlich machten.
Die Vertreter der Datenschutzbeauftragten stellten allerdings auch nicht in Abrede, dass für einzelne Geschäftsbereiche und konkret beschriebene Zwecke differenzierte Sicherheitskonzepte mit detaillierter Begründung für eine zulässige Videoüberwachung denkbar seien. Grundlage hierfür müssten entsprechende Analysen und die Berücksichtigung der gesetzlich gebotenen Interessenabwägung und des Grundsatzes der Verhältnismäßigkeit sein. Die Begründung solle sich insbesondere auch auf die zeitliche und räumliche Ausdehnung der Überwachung beziehen.

Präventive Wirkung entfaltet eine Videoüberwachung nur durch ein Monitoring mit unmittelbarer Krisenintervention

Zweck festlegen und Alternativen prüfen

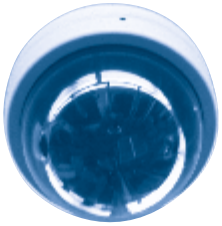
Die Behauptung, eine Videoüberwachung sei vor dem Hintergrund allgemeiner Informationen über eine Zunahme von Überfällen zur Steigerung des Sicherheitsgefühls angezeigt, stelle keine konkrete Zweckfestlegung für eine erforderliche Videoüberwachung dar. Eine zulässige Zweckfestlegung müsse im Übrigen bei der Durchführung der jeweiligen Videoüberwachungsmaßnahme konsequent beachtet und umgesetzt werden. Zudem müssten in jedem Einzelfall Alternativen unter Berücksichtigung auch der Kosten für die notwendigen begleitenden Maßnahmen geprüft und in die datenschutzrechtliche Bewertung einbezogen werden. Zu berücksichtigen sei auch, dass die Videoüberwachung nur ein Element eines stimmigen Sicherheitskonzepts zum Schutz der Beschäftigten sein könne. Sie lasse sich durch andere Maßnahmen unterstützen, wie etwa eine Verstärkung des bargeldlosen Zahlungsverkehrs mit transparenter Information nach außen, aber auch im gegebenenfalls notwendigen Umfang einschränken. Die Vertreter der Datenschutzbeauftragten verwiesen weiter darauf, dass die Einschätzung einer bestimmten, eine Videoüberwachung rechtfertigenden Gefährdungslage in zeitlichen Abständen von etwa sechs Monaten zu überprüfen sei. Hierbei müsse auch die wesentliche Frage berücksichtigt werden, ob weitere Straftaten verübt worden seien, die Anlass für eine Fortführung der Videoüberwachung sein könnten.

Mittlerweile wandert im Bereich der Tankstellen das Bargeld vielfach in einen Automaten, der auch das Wechselgeld herausgibt. Die Kassetten können von Mitarbeitern nicht geöffnet werden. Eine Videoüberwachung ist hier also entbehrlich.

Verbandsmitglieder besser informieren

Im Hinblick auf die besondere Bedeutung der konkreten Umstände im Einzelfall für die grundsätzliche Zulässigkeit der jeweiligen Videoüberwachung empfahlen die Vertreter der Datenschutzbeauftragten dem HDE, seine Mitglieder umfänglich über die datenschutzrechtlichen Voraussetzungen der Videoüberwachung in geeigneter Weise zu informieren. Sofern einzelne Unternehmen Beratungsbedarf zu datenschutzrechtlichen Fragen der Videoüberwachung hätten, der nicht betriebsintern – etwa im Wege der Prüfung durch die/den betrieblichen Datenschutzbeauftragte/n – geklärt werden könne, seien die jeweiligen Datenschutzaufsichtsbehörden die geeigneten Ansprechpartner.

Video-überwachung in Fitnessstudios: Kameras auch im Kinderclub



Auch in Freizeiteinrichtungen gibt es immer mehr Videoüberwachung. Eingaben dazu erreichten mich von Mitgliedern mehrerer Fitnessstudios. In einem Fall gab es Hinweise auf eine umfassende Kamerainstallation, die selbst vor dem Saunabereich nicht haltmachte. Bei der Prüfung stellte sich heraus, dass zusätzlich zu den Wellnessbereichen unter anderem auch die Eingangsbereiche, die Trainingsfläche, der Kursraum und der Kinderclub überwacht wurden. Insgesamt handelte es sich um 12 Kameras.

Als Begründung für die Kameras wurde pauschal der Schutz vor Diebstahl, Vandalismus, das Hausrecht und die Wahrung der Sicherheit der Kundschaft in Bereichen genannt, in denen kein Personal anwesend ist. Allerdings konnte der Betreiber keine konkreten Vorfälle darlegen oder glaubhaft machen, welche die umfassende Videoüberwachung mit dieser Zweckbestimmung hätten rechtfertigen können (siehe hierzu auch die grundlegenden Ausführungen in meinem XX. Tätigkeitsbericht, S. 114 f.).
Die geltend gemachten Gründe reichten somit nicht aus, um diese umfangreiche und das Persönlichkeitsrecht der Studiobesucher empfindlich beeinträchtigende Videoüberwachung zu legitimieren. Da die in § 6b Bundesdatenschutzgesetz (BDSG) enthaltenen Voraussetzungen für eine zulässige Videoüberwachung daher eindeutig nicht vorlagen, erwirkte ich bereits im Rahmen meiner Prüfung eine zunächst vorläufige Abschaltung der Anlage. Nachdem auch ein von dem Betreiber der Videoüberwachungsanlage zwischenzeitlich eingeschaltetes Fachunternehmen für Datenschutz und IT-Sicherheit die Videoanlage begutachtet und meine rechtliche Einschätzung bestätigt hatte, demontierte der Betreiber die Anlage komplett. Dazu hatte ihn auch der Umstand bewogen, dass er einen betrieblichen Datenschutzbeauftragten hätte bestellen müssen, um überhaupt Kameras in seinem Fitnessstudio betreiben zu können.

Videoüberwachungen, die besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, unterliegen der Vorabkontrolle nach § 4d Abs. 5 BDSG, die gemäß 4d Abs. 6 BDSG vom betrieblichen Datenschutzbeauftragten zu erstellen ist. Solche besonderen Risiken liegen vor, wenn Überwachungskameras nicht punktuell, sondern von der verantwortlichen Stelle in größerer Zahl und zentral kontrolliert werden.

Videoüberwachung in und an Fahrzeugen: In Taxis nur eingeschränkt, außen gar nicht

Angriffe auf Taxifahrer und der Raub oder die Erpressung der Tageskasse sind leider ein häufiges Kriminalitätsphänomen. Um sich davor zu schützen und Straftaten besser aufklären zu können, trat der Deutsche Taxi- und Mietwagenverband e. V. an die Datenschutzaufsichtsbehören mit der Frage heran, ob zur Reduzierung dieser Risiken der Einsatz von Videokameras in Taxis datenschutzrechtlich denkbar sei. Zeitgleich fragte ein großes Versicherungsunternehmen bei der zuständigen Aufsichtsbehörde an, ob zusätzlich zu einer Videoüberwachung in Taxis auch die Verwendung von Taxenunfallkameras, sogenannten Dash Cams, zulässig sei.

Solche zum Beispiel an der Frontscheibe der Fahrzeuge installierte Kameras sollten nach der Vorstellung der Versicherung das Fahrverhalten der Taxifahrer beeinflussen und gleichzeitig kritische Verkehrssituationen und Unfälle nachvollziehbar dokumentieren. Mit diesen Unfallkameras sollte es letztlich ermöglicht werden, neue und die Versicherungsbeiträge reduzierende Tarife anbieten zu können.

Ständige Überwachung in Taxis unzulässig

Wie bei vielen länderübergreifenden Themen haben auch hier die Datenschutzaufsichtsbehörden eine gemeinsame und einvernehmliche datenschutzrechtliche Beurteilung vorgenommen und dazu einen aktuellen Beschluss gefasst. Bei der Beurteilung war folgendes zu berücksichtigen:
Die Zulässigkeit einer Videoüberwachung durch Taxiunternehmen bestimmt sich nach § 6b Bundesdatenschutzgesetz (BDSG). Gemäß § 6b Abs. 1 Nr. 3, Abs. 3 BDSG ist eine Beobachtung und Aufzeichnung mittels Videokameras nur zulässig, soweit dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das betroffene Taxiunternehmen muss als verantwortliche Stelle vorrangig alternative und weniger einschneidende Schutzmaßnahmen in Betracht ziehen, bevor eine uneingeschränkte Videoüberwachung des Fahrgastraumes erwogen werden kann. Hier sind beispielsweise die Möglichkeit des anlassbezogenen Auslösens eines „stillen Alarms“ oder eines GPS-gestützten Notrufsignals zu nennen. Dieser in Taxis ohnehin vorhandene Notrufknopf kann mit der Videoanlage so verbunden werden, dass die Videoaufzeichnung zeitgleich mit der Aussendung des Notrufsignals beginnt. Der Fahrer kann somit selbst entscheiden, ob nach seiner Einschätzung eine bedrohliche Situation gegeben ist und es mithin einen Anlass für die Aufzeichnung gibt.
Eine anlasslose Videoüberwachung, die ohne Einflussnahmemöglichkeit des Fahrers generell und automatisch einsetzt und bei der während des gesamten Beförderungsvorgangs sowohl die Fahrgäste als auch das gesamte Geschehen im Fahrgastbereich aufgezeichnet werden, ist dagegen weder erforderlich noch verhältnismäßig. Unter Berücksichtigung sowohl der Sicherheitsinteressen des Fahrpersonals als auch der Persönlichkeitsrechte der betroffenen Fahrgäste ist die automatische Videoaufzeichnung

vielmehr auf das Anfertigen einzelner Standbilder der Fahrgäste beim Einsteigen oder einer kurzen Videosequenz von längstens 15 Sekunden vor Fahrtbeginn zu beschränken. Aber auch diese Bilder sind gemäß § 6b Abs. 5 BDSG unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind. Gab es kein Schadensereignis, sind die Bildaufnahmen der Innenkameras im Regelfall innerhalb von 24 Stunden, spätestens aber nach 48 Stunden zu löschen.

Im Übrigen müssen potentielle Fahrgäste entsprechend dem Transparenzgebot des § 6b Abs. 2 BDSG vor dem Einsteigen durch deutlich sichtbare Beschilderungen an den Fahrgasttüren auf den Umstand der Videoüberwachung und die hierfür verantwortliche Stelle hingewiesen werden. Schließlich haben die Taxi-Unternehmen durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass nur berechtigten Personen ein Zugriff auf die Bildaufzeichnungen möglich und ein unbefugtes Auslesen der Daten ausgeschlossen ist.

Eine anlasslose Videoüberwachung während des gesamten Beförderungsvorgangs ist weder erforderlich noch verhältnismäßig.

Betrieb von „Dash Cams“ ohne Rechtsgrundlage

Die Voraussetzungen des § 6b Abs. 1, Abs. 3 BDSG sind bei den sogenannten Dash Cams, mit denen der öffentliche Verkehrsraum – etwa zur vorsorglichen beweissichernden Dokumentation für den Fall eines Schadensereignisses – einer Überwachung unterzogen wird, nicht erfüllt. Unerheblich ist dabei, ob die Kameras mobil sind und eventuell nur die nähere Umgebung des Taxis oder Privat-Kraftfahrzeugs erfassen. Mit derartigen Kameras sollen gezielt personenbezogene Daten (Personen, Kfz-Kennzeichen, Aufschriften auf Fahrzeugen etc.) erhoben werden, um später anhand der Aufnahmen beispielsweise Verantwortlichkeiten von Verkehrsteilnehmern und Haftungsfragen klären zu können. Das Recht auf informationelle Selbstbestimmung umfasst jedoch die Möglichkeit, sich in der Öffentlichkeit frei und ungezwungen zu bewegen, ohne befürchten zu müssen, ungewollt und ohne Anlass zum Objekt einer Videoüberwachung zu werden. Eine Rechtsgrundlage für diese Datenerhebung gibt es nicht. Insbesondere kann die Videoüberwachung des allgemeinen Verkehrsgeschehens mittels Dash Cams auf keinen der in § 6b Abs. 1 BDSG genannten Zwecke gestützt werden, so dass sie bereits aus diesem Grund unzulässig ist.

So scheidet eine Wahrnehmung des Hausrechts (Abs. 1 Nr. 2) aus, da das Hausrecht am Auto nicht auch das Recht umfasst, sämtliche öffentlichen Verkehrsflächen (Straßen, Wege, Parkplätze) durch die Videoüberwachung zu erfassen. Aber auch der nach der Gesetzesbegründung ohnehin eng auszulegende Ausnahmetatbestand der „Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ (Abs. 1 Nr. 3) kommt nicht in Betracht. Ein hier allein in Betracht zu ziehendes berechtigtes Interesse des Taxiunternehmens ist allenfalls vorstellbar, wenn dieses in seiner Eigenschaft als Kfz-Halter betroffen ist. Soweit es allgemein um die Aufklärung von „kritischen Verkehrssituationen“ wie Geschwindigkeits- oder Rotlichtverstöße sowie andere Verkehrsordnungswidrigkeiten geht, treffen deren Konsequenzen in aller Regel aber ausschließlich die Taxifahrer. Erst recht gibt es kein berechtigtes Interesse des Taxiunternehmens, die Aufzeichnung des Verkehrsgeschehens zur permanenten Überwachung der angestellten Taxifahrer zu nutzen und sich mit Hilfe der Aufnahmen ein Bild von dem Fahrverhalten der Beschäftigten zu machen, um zum Beispiel riskante Fahrweisen aufzudecken. Dabei ist auch zu berücksichtigen, dass selbst die Polizei Videokameras zur Verfolgung von Straftaten und Ordnungswidrigkeiten gemäß §§ 100 h

Weder Unternehmen noch Einzelpersonen können eine Videoüberwachung zur Wahrnehmung vermeintlich eigener berechtigter Interessen in einem Umfang durchführen, der ausschließlich öffentlichen Stellen unter strengen Voraussetzungen erlaubt ist.

Abs. 1 Nr. 1, 163 b Abs. 1 Satz 1 Strafprozessordnung (StPO) in Verbindung mit § 46 Abs. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) nur einsetzen darf, wenn gegen den von der Videoaufzeichnung betroffenen Kfz-Führer der Anfangsverdacht einer Straftat oder Ordnungswidrigkeit besteht. Erst wenn ein solcher Verdacht vorliegt, dürfen entsprechende Videoaufzeichnungssysteme überhaupt aktiviert werden. Dies hat auch das Bundesverfassungsgericht in seiner Entscheidung vom 11.8.2009 (Az.: 2 BvR 941/08) zur Zulässigkeit verdachtsunabhängiger Verkehrskontrollen mit Videoüberwachung zum Nachweis von Abstandsverstößen ausdrücklich bestätigt.

Außenkameras stellen alle Verkehrsteilnehmer unter Generalverdacht

Abgesehen vom Fehlen eines zulässigen Zwecks wäre eine Videoüberwachung mittels Dash Cams an Taxis oder sonstigen Kraftfahrzeugen zudem weder erforderlich noch verhältnismäßig und auch aus diesen Gründen unzulässig. Es ist nämlich nicht ersichtlich, dass im Schadensfall polizeiliche Ermittlungen, Spurensicherung und Zeugenbeweise zur Erreichung der mit den Außenkameras verfolgten Zwecken nicht ausreichten. Zudem gibt es gewichtige Anhaltspunkte dafür, dass schutzwürdige Interessen der Betroffenen – sowohl der angestellten Taxi-Fahrer als auch der übrigen Verkehrsteilnehmer – überwiegen. Abgesehen von dem berechtigten Interesse des Fahrers, nicht einer permanenten Verhaltens- und Leistungskontrolle ausgesetzt zu sein, wird auch das Recht auf informationelle Selbstbestimmung der übrigen Verkehrsteilnehmer durch Dash Cams empfindlich beeinträchtigt, wenn mit solchen Kameras ausgestattete Taxis oder privat genutzte Kraftfahrzeuge wesentliche Teile des vor und neben diesen Fahrzeugen befindlichen Straßenverkehrs erfassen. Auf diese Weise würden andere Verkehrsteilnehmer unweigerlich und unvermeidbar in den Aufnahmebereich der Kameras geraten. Hinzu kommt, dass die Außenkameras für sie regelmäßig nicht zu erkennen sein dürften, so dass aus ihrer Sicht eine versteckte Videoüberwachung erfolgen würde. Sämtliche Verkehrsteilnehmer würden dabei bereits präventiv im Vorgriff auf einen potentiellen Schadensfall erfasst und mithin in unverhältnismäßiger Weise unter Generalverdacht gestellt. All dies ist unter Datenschutzgesichtspunkten inakzeptabel.
Die Ausstattung von Taxis mit Unfallkameras, die von dem Versicherungsunternehmen als Grundlage eines neuen Versicherungstarifs vorgesehen war, ist daher unzulässig. Dieses mit allen Aufsichtsbehörden abgestimmte Prüfungsergebnis ist zwischenzeitlich dem Kfz-Versicherer mitgeteilt worden. Die in anderen Staaten bei der Bildung von Kfz-Versicherungstarifen bereits praktizierte und tarifmindernde Berücksichtigung von Unfallkameras wird in Deutschland ohne Verstoß gegen den Datenschutz also nicht möglich sein.

Weitere Informationen:

Beschluss des Düsseldorfer Kreises zu „Videoüberwachung in und an Taxis“:
www.bfdi.bund.de >Datenschutz >Entschließungen >Düsseldorfer Kreis

Videoüberwachung in Schwimmbädern: Verbotenes Auge vor der Sauna

Immer wieder erhalte ich Eingaben von erbosten Schwimmbadgästen, die sich über Videokameras in den Umkleidebereichen, in Zugängen zu Saunabereichen oder an Rutschen und anderen Wasserspielgeräten von Schwimmbädern beschweren. Sie empfinden die Überwachung besonders der sensiblen Bereiche zumeist als unverhältnismäßigen Eingriff in ihre Privatsphäre oder schlicht als unzulässig.

Da solche Beschwerden besonders im aktuellen Berichtszeitraum zugenommen haben, habe ich eine Reihe von Bädern überprüft. Videoüberwachungsanlagen werden in Schwimmbädern zur Verfolgung verschiedener Zwecke eingesetzt. Dabei habe ich im Rahmen meiner Prüfungen stets kritisch hinterfragt, ob der Schwimmbadbetreiber tatsächlich Zwecke verfolgt, die das Bundesdatenschutzgesetz (BDSG) in § 6b Abs. 1 billigt und die gerade der Badbetreiber verfolgen darf. Einige Fälle gaben hier Anlass zu Zweifeln, da die Kameras vor allem in den eigentlichen Schwimmbeckenbereichen ganz offenkundig in erster Linie dazu genutzt wurden, die Schwimmbadaufsicht personell zu reduzieren. Der Einsatz von Kameras zur Personaleinsparung in diesen sensiblen Bereichen der sogenannten Wasseraufsicht ist jedoch bereits nach dem Regelwerk (R 94.05) der Deutschen Gesellschaft für das Badewesen e.V. unzulässig. Eine Videoüberwachung des Wasserbereichs kann deshalb auch datenschutzrechtlich allenfalls zur Unterstützung der Wasseraufsicht in schlecht einsehbaren Beckenbereichen, und dann auch nur als reine Monitorlösung, also ohne Aufzeichnung der Videobilder, in Betracht kommen.

Kein Kameraeinsatz zur Einsparung von Personal der Wasseraufsicht, sondern nur als Monitoring zur Unterstützung ihrer Aufgaben.

Nur wenige verfolgte Zwecke sind datenschutzkonform

Im Übrigen ist wie bei jedem Einsatz von Videoüberwachungstechnik immer zu prüfen, ob die Kameras zur Erfüllung des von der verantwortlichen Stelle jeweils genannten Zwecks erforderlich sind und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Hinsichtlich der in § 6b Abs. 1 Nrn. 2 und 3 BDSG genannten zulässigen Zwecke einer Videoüberwachung ergaben meine Kontrollen der Schwimmbäder im Übrigen folgendes Bild:

1. Wahrnehmung des Hausrechts

Die Videoüberwachung ist zur Wahrnehmung des Hausrechts nach § 6b Abs. 1 Nr. 2 BDSG jedenfalls während der Öffnungszeiten des Schwimmbades in aller Regel nicht erforderlich. Vielmehr kann dieser Zweck auch durch andere Mittel, wie beispielsweise Kontrollen des Personals oder Zutrittsbeschränkungen durch Dreh-

kreuze, erreicht werden. In Einzelfällen kann eine zulässige Videoüberwachung aber in Betracht kommen, wenn es im Rahmen des Hausrechts zum Beispiel um den Schutz der Badegäste vor Übergriffen in schlecht einsehbaren Bereichen geht. So hatte ich im Rahmen der Prüfung eines Erlebnisbades die Zulässigkeit von nicht weniger als 28 Kameras zu beurteilen, welche die Spind- und Umkleidebereiche vollständig erfassten. Die Badegäste durchschritten diese Bereiche nicht nur kurz, sondern hielten sich in ihnen zu Umkleidezwecken längere Zeit auf. Einige trugen dabei nur Badekleidung oder Unterwäsche. Ferner stellte ich fest, dass sich die Badegäste an Spiegeln, die im überwachten Bereich an Säulen befestigt waren, auch frisierten. Die Videodaten wurden allerdings ausschließlich aufgezeichnet; ein Monitoring, das allein eine umgehende Interventionsmöglichkeit eröffnet hätte, fand dagegen nicht statt.

Eine reine Videoaufzeichnung mit anschließender Bildauswertung nach begangener Straftat dient der effektiven Ausübung des Hausrechts nicht und ist daher zur Erreichung dieses Zwecks ungeeignet.

Dementsprechend benannte der Badbetreiber als Zweck dieser umfassenden Videoüberwachung auch nur die (repressive) Verfolgung von Straftaten, ein präventiver Schutz der Badegäste vor Diebstahl und Übergriffen sollte dagegen mit den Kameras nicht erreicht werden.

Mit dieser Zweckbestimmung durften die 28 Kameras in der vorgefundenen „blackbox"-Ausgestaltung allerdings nicht betrieben werden. Denn die Voraussetzungen des § 6b BDSG waren nicht erfüllt, da die Kameras ausdrücklich nicht der Wahrnehmung des Hausrechts (§ 6b Abs. 1 Nr. 2 BDSG) dienen sollten. Nur mit der effektiven Ausübung des Hausrechts kann aber sichergestellt werden, dass Verstöße gegen die Haus- oder Badeordnung, die in aller Regel auch den Schutz mitgebrachten Eigentums befugter Besucher/Badegäste sowie deren Schutz vor Übergriffen zum Ziel hat, unterbunden werden. Dies ist, bezogen auf nicht einsehbare Spind- und Umkleidebereiche, ausschließlich mit einer Monitoring-gestützten Videoüberwachung möglich. Denn nur durch die Beobachtung in Echtzeit kann Verstößen gegen die Hausordnung durch unmittelbar folgende geeignete Intervention begegnet werden. Eine daneben durchgeführte Aufzeichnung der Videobilder kommt allenfalls in Betracht, sobald aufgrund der Beobachtung Straftaten festgestellt wurden und die Aufzeichnung zu Beweiszwecken verwendet werden kann und soll.

Generell ist bei Aufzeichnungen von Videobildern aus Schwimmbädern aber strikte Zurückhaltung geboten, weil vor dem Hintergrund der oben dargestellten typischen Verhaltensweisen der Badegäste im Spind- und Umkleidebereich davon auszugehen ist, dass schutzwürdige Interessen der von der Videoüberwachung Betroffenen überwiegen. Hier liegt eine Situation vor, die mit der in Toilettenvorräumen und Duschen vergleichbar ist. Derartige Bereiche sind jedoch generell jeglicher Videoüberwachung entzogen, so dass die schutzwürdigen Interessen der von Videoüberwachung im Spind- und Umkleidebereich betroffenen Badegäste nur dann zurückzustehen haben, wenn der Schutz überragender Rechtsgüter auch eine Aufzeichnung dieser Bilder erfordert. Dies wird aber nur in seltenen Ausnahmefällen anzunehmen sein.

2. Wahrnehmung berechtigter Interessen

Als berechtigte Interessen kommen nur solche in Betracht, die dem Interessenkreis der verantwortlichen Stelle zugeordnet werden können und deshalb auch nur von dieser befugt verfolgt werden können. Gleichwohl wird von Schwimmbadbetreibern als Zweckbestimmung der von ihnen verwendeten Videoüberwachung bisweilen auch die Unterstützung bei der Klärung von Haftungsfragen der Badbesucher untereinander genannt, obwohl die Klärung von juristischen Streitigkeiten der Kunden nicht Aufgabe des Badbetreibers ist und kein berechtigtes Interesse im Sinne des § 6b Abs. 1 Nr. 3 BDSG darstellt. Auch die immer wieder als Zweck genannte Abwehr von Haftungsansprüchen gegen den Betreiber rechtfertigt eine Videoüberwachung bestimmter Gefahrenbereiche eines Bades nicht. Zwar mag es sich dabei um berechtigte Interessen im Sinne von § 6b Abs. 1 Nr. 3 BDSG handeln. Eine hier zumeist ausschließliche Videoaufzeichnung ist aber als Beweismittel zur Abwehr von Haftungsansprüchen nicht erforderlich, was auch in der zivilrechtlichen Rechtsprechung anerkannt ist (u. a. OLG Koblenz, Beschlüsse vom 26.4.2010, Az. 1 W 200/10, und vom 7.5.2010, Az. 8 U 810/09). Denkbar ist jedoch eine punktuelle Videoüberwachung von erfahrungsgemäß unfallträchtigen Bereichen wie zum Beispiel Wasserrutschen, wenn die Überwachung als reines Monitoring ausgestaltet ist und zum Ziel hat, kritischem Verhalten von Badegästen umgehend begegnen zu können.

Klärung von juristischen Streitigkeiten der Kunden ist nicht Aufgabe des Badbetreibers.

Badbetreiber kein polizeiliches Hilfsorgan

Im Rahmen meiner Prüfungen nannten mir einige Badbetreiber schließlich auch den Zweck der Unterstützung polizeilicher Straftatenaufklärung mit Hilfe der Überwachungskameras ihres Schwimmbades. Solchen Schwimmbadbetreibern begegnete ich mit dem Hinweis, dass sie sich offenbar nur als polizeiliches Hilfsorgan zur Unterstützung staatlicher Gefahrenabwehr und Strafrechtspflege begreifen und damit keine berechtigten eigenen Interessen im oben beschriebenen Sinn verfolgen, denn die Aufklärung von Straftaten ist Aufgabe der Strafverfolgungsbehörden und nicht die eines Schwimmbadbetreibers.

Monitore im Eingangsbereich von Geschäften: Passanten schauen beim Einkaufen zu

Im Zusammenhang mit einer Eingabe stellte sich die Frage, ob Monitore im Eingangsbereich, auf denen die Kunden sich selbst beim Betreten eines Geschäfts oder andere Kunden in überwachten Bereichen mit möglicherweise wechselnden Einstellungen sehen können, datenschutzrechtlich zulässig sind.

Diese Monitore dienen nicht der eigentlichen Videoüberwachung durch das Unternehmen, sondern sind als Hinweis an die Kunden gerichtet, die – sollten sie Hinweisschilder nicht sehen – erkennen können, dass und gegebenenfalls welche Bereiche videoüberwacht werden. Die Monitore sollen daher auch eine abschreckende Wirkung haben. Als einziger Hinweis auf die Videoüberwachung reichen derartige Monitore allerdings nicht aus, sondern es sind zusätzlich Hinweisschilder nach § 6b Abs. 2 Bundesdatenschutzgesetz (BDSG) anzubringen, welche die betroffenen Kunden vor Eintritt in den Erfassungsbereich der Kameras auf die Videoüberwachung hinweisen.

Zudem war der hier begutachtete Monitor aufgrund seiner Darstellung aktueller Aufnahmen aus den videoüberwachten Bereichen datenschutzrechtlich unzulässig, da schutzwürdige Interessen der Kunden entgegenstanden. Denn aufgrund der Anbringung des Monitors am Geschäftseingang sind bereits beim Verweilen vor dem Ladenlokal und erst recht nach Betreten des Geschäfts die Kunden auf dem Monitor sichtbar. Dadurch ist es möglich, laufend andere Kunden und Bedienvorgänge des Ladenpersonals zu beobachten, ohne dass diese bemerken, wer sie ansieht. Dies stellt einen unzulässigen Eingriff in das Persönlichkeitsrecht dar. Zudem mangelt es hier bereits an einem berechtigten Interesse der verantwortlichen Stelle im Sinne des § 6b Abs. 1 Nr. 3 BDSG und an der Erforderlichkeit der Maßnahme.

Zulässig wäre ein Monitor im Eingangsbereich, bei dem keine wechselnde Einstellungen von Kunden in den verschiedenen überwachten Bereichen erscheinen, sondern statisch der Eingangsbereich abgebildet würde, ohne Speicherung der Bilddaten.

Einer solchen Lösung ständen schutzwürdige Interessen der Kunden an einer Überwachung nicht entgegen, der beabsichtigte Warneffekt bestünde aber weiterhin.

Die Tulpe im Fokus der Kamera:
Blumenhändler überwacht Pflanzen und Mitarbeiter

Im 16. und 17. Jahrhundert wurde Tulpen zu einem Spekulationsobjekt, für die in der Hochzeit mehrere Tausend Gulden gezahlt wurden. So wurde die Tulpe auch zu einem begehrten, weil kostbaren Diebesgut. Doch obwohl sich seit dem Börsenkrach von 1637 der Handelswert von Tulpen wieder normalisiert hat, ließ ein Blumenhändler seine 15 Filialen mit Videokameras überwachen. Dabei wurde als Zweck auch der Warendiebstahl benannt.

Im Rahmen meiner Prüfung stellte ich fest, dass die Videoüberwachung jedoch weder formell, noch materiell den Anforderungen des Bundesdatenschutzgesetzes (BDSG) entsprach. So wurden die Videobilder erst dann überschrieben, wenn die Festplatte voll war. Ein festgelegter Zeitraum für die Löschung der Daten existierte nicht. Dies widersprach dem Löschungsgebot aus § 6b Abs. 5 BDSG. Ich forderte das Unternehmen daher auf, die Speicherdauer auf maximal 72 Stunden zu begrenzen. Dem Löschungsgebot wird dabei am wirksamsten durch eine automatisierte periodische Löschung entsprochen, etwa durch Selbstüberschreiben zurückliegender Aufnahmen.
Darüber hinaus entsprachen die Hinweisschilder nicht den Anforderungen des Bundesdatenschutzgesetzes, sondern waren um die Angabe der verantwortlichen Stelle zu ergänzen und in allen Fällen so zu platzieren, dass sie vor Betreten des überwachten Bereichs wahrnehmbar sind. Zudem war die Verfahrensbeschreibung unvollständig, denn es fehlten die Angaben der technisch-organisatorischen Maßnahmen zum Schutz der Daten.
Bei den mir vorgelegten Videografien stellte sich in allen Fällen zunächst die grundsätzliche Frage der Erforderlichkeit. Außerdem wurden in mehreren Filialen explizit auch die Arbeitsbereiche der Mitarbeiterinnen und Mitarbeiter überwacht, was eine datenschutzrechtlich unzulässige Arbeits- und Leistungskontrolle ermöglichte und somit rechtswidrig war.
In der Folge verzichtete das Unternehmen auf die Aufzeichnung der Daten und änderte zudem die Erfassungsbereiche mehrerer Kameras. Es wurde eine überarbeitete Verfahrensbeschreibung vorgelegt, die nun den datenschutzrechtlichen Anforderungen entsprach. Schließlich wurden die Hinweisschilder neu gestaltet und aufgehängt. Nach vielen Gesprächen und einer regen Korrespondenz konnte ich bewirken, dass die Videoüberwachung nunmehr den Anforderungen des Bundesdatenschutzgesetzes entspricht.

Speicherdauer der Videobilder maximal 72 Stunden, danach Überschreibung.

Betriebliche Datenschutzbeauftragte: Entfällt die Pflicht für kleine Firmen?

Nicht-öffentliche Stellen, also natürliche Personen, Firmen und andere Personenvereinigungen des privaten Rechts, die personenbezogene Daten automatisiert verarbeiten, sind nach dem Bundesdatenschutzgesetz (BDSG) verpflichtet, dem Landesbeauftragten für den Datenschutz Niedersachsen als zuständige Datenschutzaufsichtsbehörde die Verfahren vor ihrer Inbetriebnahme zu melden. Die Meldepflicht entfällt, wenn ein Beauftragter für den Datenschutz bestellt wird. Im von der EU-Kommission am 25.1.2012 vorgelegten Entwurf einer Datenschutz-Grundverordnung wird erstmals eine europarechtliche Verpflichtung zur Bestellung von Datenschutzbeauftragten in Wirtschaft und Verwaltung vorgesehen.

Anfragen der täglichen Praxis spiegeln jedoch wider, dass bei vielen betrieblichen und vorrangig bei externen Datenschutzbeauftragten Unsicherheit darüber herrscht, ob und wie sich die Bestellung eines betrieblichen Datenschutzbeauftragten vor dem Hintergrund der geplanten EU-Verordnung auswirken wird. Beispielsweise wird aufgrund der im Verordnungsentwurf genannten Bestelldauer von nur zwei Jahren die Gefahr gesehen, dass durch die geringe Laufzeit eine effektive und im Einzelfall kritische Wahrnehmung der Aufgaben verhindert wird. Auch die in dem Entwurf genannte Untergrenze für die Pflichtbestellung eines Datenschutzbeauftragten von 250 in einem Unternehmen beschäftigten Mitarbeitern verbreitet große Unruhe bei den Datenschutzbeauftragten. Vielfach sind Unternehmen mit deutlich weniger Mitarbeitern verstärkt mit der Verarbeitung personenbezogener Daten befasst. Diese Unternehmen könnten dann unter Umständen auf die Investition in den Datenschutzbeauftragten verzichten.

Ein **Beauftragter für den Datenschutz** gem. § 4f Abs. 1 BDSG ist zu bestellen, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind

Einsichtsrecht für jedermann

Nach § 4 Abs. 1 BDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Die verantwortlichen Stellen im nicht-öffentlichen Bereich haben eine Übersicht über ihre automatisierten Verarbeitungen personenbezogener Daten zu führen. Diese Übersicht darf jedermann unentgeltlich einsehen. Im Verfahrensverzeichnis ist daher zu dokumentieren, ob die Verarbeitung aufgrund einer Einwilligung oder einer Rechtsvorschrift erfolgt. Diese Angaben sind für jedes Verfahren separat darzulegen. Das Verfahren ist dabei eindeutig zu bezeichnen. Über die Bezeichnung muss sich das Verfahren im Datenverarbeitungssystem der verantwortlichen Stelle identifizieren lassen. Der Zweck der Datenverarbeitung ist so präzise wie möglich zu benennen. Es ist Aufgabe der betrieblichen Datenschutzbeauftragten, auf Antrag die Angaben in dem Verfahrensverzeichnis den Antragstellern in geeigneter Weise verfügbar zu machen. Auch nicht-öffentli-

che Stellen ohne betrieblichen Datenschutzbeauftragten müssen eine entsprechende Übersicht führen und zur Einsicht bereithalten. Bis auf die allgemeine Beschreibung, die es ermöglicht, die Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu beurteilen, sind alle Angaben öffentlich.

Vorschriften des BDSG oft nicht bekannt

Im Berichtszeitraum führte ich bei niedersächsischen Unternehmen unterschiedlicher Branchen insgesamt elf Kontrollen gemäß § 38 Abs. 2 BDSG durch. Dabei verlangten meine Mitarbeiterinnen und Mitarbeiter die Vorlage des Verfahrensverzeichnisses (§ 4g Abs. 2 BDSG). Insbesondere bei Unternehmen, die aufgrund der Größe des Unternehmens keinen Datenschutzbeauftragten bestellen müssen, stellte ich immer wieder fest, dass die Verfahrensverzeichnisse gar nicht oder nur unzureichend vorhanden waren. Hinzu kommt, dass der Mehrzahl der Unternehmen die Vorschriften des BDSG nicht einmal bekannt waren. Mein Webangebot enthält zahlreiche Informationen. Allerdings mussten von mir immer wieder zusätzliche Hilfestellungen zur Erstellung des Verfahrensverzeichnisses gegeben werden. Wünschenswert wäre es, bei der Gründung von Unternehmen zum Beispiel bei der Gewerbeanmeldung oder auch bei Schulungen für Existenzgründer auf die entsprechenden Vorschriften hinzuweisen und damit auch gleichzeitig die Aufmerksamkeit für den Datenschutz zu erhöhen.

Inhalt der Meldepflicht bzw. des Verfahrensverzeichnisses (§ 4e i. V. m. § 4g Abs. 2 BDSG):

1. Name oder Firma der verantwortlichen Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Weitere Informationen:

www.lfd-niedersachsen.de
>Technik und Organisation >
Verfahrensregister und Verfahrensverzeichnis nach BDSG

Datenschutz in den Medien: Freiwillige Selbstkontrolle statt staatlicher Aufsicht

In Zeitungsartikeln werden regelmäßig Personen mit vollem Namen genannt, dabei stellt sich die Frage nach dem Datenschutz. Von Bedeutung ist in diesem Zusammenhang das so genannte Medienprivileg, wonach die Medien datenschutzrechtlich besonders zu behandeln sind.

Bundesdatenschutzgesetz nicht anwendbar

Die grundgesetzlich geschützte Pressefreiheit befreit die Medien weitestgehend von der Einhaltung der datenschutzrechtlichen Vorschriften. Dies beruht auch auf Art. 9 Abs. 1 S. 2 der EU-Datenschutzrichtlinie. Zweck dieser Sonderbehandlung von Presseunternehmen ist die Ermöglichung einer freien Berichterstattung ohne staatliche Einmischung. Erfolgt eine Datenverarbeitung in der Presse ausschließlich zu eigenen journalistisch-redaktionellen Zwecken, sind die zentralen Regelungen des Bundesdatenschutzgesetzes (BDSG) nicht anwendbar (§ 41 BDSG in Verbindung mit § 19 Niedersächsisches Pressegesetz). Insbesondere muss die Datenverarbeitung nicht wie sonst vorgeschrieben auf einer Rechtsgrundlage nach dem BDSG oder einer Einwilligung der betroffenen Person beruhen. Auch besteht nach dem BDSG kein Anspruch der betroffenen Person auf Auskunft oder auf Löschung/Sperrung/Berichtigung der Daten.
Das Medienprivileg gilt nur für den journalistisch-redaktionellen Bereich. Ausschlaggebend ist bei der Datenverarbeitung die Absicht der verantwortliche Stelle zur Veröffentlichung von Inhalten für einen unbestimmten Personenkreis sowie eine redaktionelle Bearbeitung. Typischerweise erfüllen Recherche, Redaktionsarbeit, die Veröffentlichung selbst, die weitere publizistische Verwertung, die Dokumentation und Archivierung von journalistischen Inhalten diese Kriterien. Dagegen können sich auch Presseunternehmen nicht auf das Medienprivileg berufen, sofern die relevante Datenverarbeitung nicht nur typischerweise bei ihnen selbst, sondern auch bei anderen Wirtschaftsunternehmen stattfindet wie zum Beispiel die Verarbeitung von Personaldaten oder die Datennutzung zu Werbezwecken.

Auch Webblogs und Internetforen begünstigt

Das Medienprivileg kann grundsätzlich auch Webblogs, Internetforen und elektronischen Tagebüchern zugute kommen. Dabei ist jedoch zu beachten, dass die genannten gesetzlichen Vorschriften kein allgemeines Medienprivileg bieten, sondern sich an der grundgesetzlich geschützten Pressefreiheit orientieren. Es kommt daher im Einzelfall darauf an, ob die genannten Veröffentlichungen durch eine journalistisch-redaktionelle Bearbeitung, die der öffentlichen Meinungsbildung dienen soll, gekennzeichnet sind, und ein gewisser Verbreitungsgrad gegeben ist.

Datenschutzaufsicht durch Presserat

Der journalistisch-redaktionelle Bereich ist nicht nur den wesentlichen Regelungen des BDSG entzogen, es gibt hier auch keine staatliche Aufsicht durch die Datenschutzaufsichtsbehörde. Die Datenschutzaufgaben werden in diesem Bereich vom Deutschen Presserat wahrnommen. Das Konzept der Datenschutzaufsicht besteht hier in einer freiwilligen Selbstkontrolle: Die Verlage können sich durch die Abgabe einer Selbstverpflichtungserklärung zur Einhaltung des Pressekodex einschließlich der dort integrierten Grundsätze zum Datenschutz verpflichten. Der Deutsche Presserat hat zum Datenschutz in Redaktionen einen Leitfaden veröffentlicht, der 2011 überarbeitet wurde.

Zahlreiche Beschwerden

Im Berichtszeitraum erreichten mich viele Beschwerden, welche die Namensnennung oder das Abdrucken von Fotos von Personen in Zeitungen betrafen. In all diesen Fällen war mir aufgrund der oben beschriebenen Regelungen ein aufsichtsbehördliches Tätigwerden verwehrt, und die Petenten mussten an den Deutschen Presserat verwiesen werden. Dies stieß bei den Petenten meist auf Unverständnis, da sich bei festgestellten Verstößen die möglichen Maßnahmen des Presserats gegen das Presseunternehmen auf Hinweise, Missbilligungen und Rügen beschränkten. Zudem sind diejenigen Presseunternehmen, die den Pressekodex nicht oder nicht mehr durch Selbstverpflichtung anerkannt haben, bei derzeitiger gesetzlicher Regelung in Niedersachsen frei von jeglicher Datenschutzkontrolle. Dies ist im letzten Jahr bei einem Fall konkret deutlich geworden, bei dem ein Presseunternehmen trotz mehrfacher Missbilligung und Rüge durch den Presserat sein datenschutzwidriges Verhalten fortsetzte und schließlich sogar den Widerruf seiner Selbstverpflichtungserklärung ankündigte. Als staatliche Aufsichtsbehörde fehlte mir hier jedoch die Befugnis zu einem Tätigwerden.

Weitere Informationen:

www.presserat.info
>Der Pressekodex >Leitfäden

Datenschutz in Europa: EU-Entwürfe stark verbesserungsbedürftig

Die aus dem Jahr 1995 stammenden EU-Vorschriften zum Datenschutz sind aufgrund des technischen Fortschritts und der Globalisierung nicht mehr zeitgemäß. Im Jahr 2012 wurden Brüssels Pläne zur bereits lang erwarteten Reform des europäischen Datenschutzrechts bekannt. Sie müssen in vielen Details verbessert werden.

Reformvorschläge der EU

Der Reformprozess begann 2010 mit der Vorstellung eines Gesamtkonzeptes zur Stärkung des Datenschutzrechts durch die EU-Kommission und der anschließenden öffentlichen Anhörung zu der von der Kommission vorgeschlagenen Überarbeitung der bisher geltenden EU-Datenschutzrichtlinie. In ihrem Konsultationsbeitrag begrüßten der Bundesbeauftragte für den Datenschutz (BfDI) und die Landesbeauftragten für den Datenschutz grundsätzlich das vorgestellte Gesamtkonzept. Am 25.1.2012 fand der Reformprozess seinen vorläufigen Höhepunkt mit der Vorstellung der geplanten Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) und der 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.

Zielrichtung

Die Datenschutzreform soll generell sowohl eine Verbesserung der Rechte des einzelnen als auch eine Stärkung des Binnenmarktes herbeiführen. Eine vorrangige Intention der EU-Kommission ist daneben die besondere Berücksichtigung des Datenschutzes im weltweiten Internet. Durch die Stärkung des Vertrauens der EU-Bürger in die digitale Wirtschaft und durch eine höhere Rechtssicherheit eines einheitlichen Rechtsrahmens innerhalb der EU erhofft sich die Kommission eine Steigerung des Wirtschaftswachstums und der Wettbewerbsfähigkeit des Binnenmarktes. Insbesondere die Richtlinie für den Bereich der Polizei und der Strafjustiz soll zu einer verbesserten Zusammenarbeit zwischen den Behörden der einzelnen Mitgliedstaaten beitragen und in ganz Europa für ein einheitlich hohes Schutzniveau sorgen.

Inhalte

Die EU-Datenschutzreform enthält folgende wesentliche Inhalte bzw. Neuerungen:

- Durch die nun gewählte Rechtsform einer Verordnung wird das Datenschutzrecht in der EU vereinheitlicht. Bisher wurde die bestehende Datenschutzrichtlinie in den einzelnen Mitgliedstaaten recht unterschiedlich umgesetzt. Dies wird durch die Verordnung mit ihrer unmittelbaren Anwendbarkeit verhindert.
- Die Datenschutzgrundverordnung soll fortan auch für Unternehmen außerhalb der EU gelten, wenn diese sich an Personen innerhalb der EU richten (Marktortprinzip).
- Die Zuständigkeit einer Datenschutzaufsichtsbehörde bestimmt sich künftig bei Unternehmen, die in mehreren Mitgliedstaaten tätig sind, nach dem Hauptsitz des Unternehmens („One-Stop-Shop“).
- Das grundsätzliche Erfordernis einer Einwilligung zu jeder Datenverarbeitung wird in der Verordnung europaweit festgeschrieben.
- Minderjährige sollen besonders geschützt werden, so ist bei Kindern bis 13 Jahren die Einwilligung gegenüber Online-Diensteanbietern unwirksam.
- Durch datenschutzfreundliche Gestaltung und Voreinstellung soll ein umfassender Datenschutz erreicht werden („privacy by design“).
- Anders als im deutschen Datenschutzrecht bisher vorgesehen, gilt die Bestellungspflicht für einen betrieblichen Datenschutzbeauftragten erst für Unternehmen mit einer Mitarbeiterzahl ab 250.
- Das nun eingeräumte „Recht auf Vergessen“ soll gewährleisten, dass personenbezogene Daten – insbesondere im Internet – gelöscht werden, wenn z. B. der Zweck ihrer Speicherung entfallen ist.
- Bürger können nach den neuen Regelungen künftig leichter auf ihre eigenen Daten zugreifen und diese bei einem Wechsel zu einem anderen Dienstleistungsanbieter mitnehmen (Recht auf Datenportabilität).

- Unternehmen trifft demnächst die Pflicht zur Benachrichtigung der Aufsichtsbehörden innerhalb von 24 Stunden bei unberechtigtem Zugriff auf personenbezogene Daten.
- Die Verordnung statuiert erweiterte Beschwerderechte von Bürgern und weitet diese auf bestimmte Organisationen aus.
- Zudem enthält die Verordnung verschärfte Sanktionsvorschriften bei Datenschutzverstößen, z. B. die Möglichkeit zur Verhängung von Bußgeldern in Höhe von bis zu 2 % des Jahresumsatzes des betreffenden Unternehmens.
- Die Verordnung sieht weiter die Bildung eines Europäischen Datenschutzausschusses vor, welcher beratend tätig werden und die einheitliche Anwendung der Verordnung sicherstellen soll.
- Die Kommission plant zusätzlich die Einführung eines in der Verordnung genau geregelten Kohärenzverfahrens (Verfahren der Zusammenarbeit der Aufsichtsbehörden in den Mitgliedstaaten und der Kommission) bei Datenverarbeitungen, die Personen in mehreren Mitgliedstaaten betreffen.
- Durch die Befugnis zur Annahme von Rechtsakten im Hinblick auf die ordnungsgemäße Anwendung der Verordnung und zur Annahme von sofort geltenden Durchführungsrechtsakten in dringlichen Fällen sowie durch besondere Befugnisse innerhalb des geplanten Kohärenzverfahrens erhält die Kommission neue Kompetenzen, z. B. die Befugnis zur Aussetzung einer geplanten Maßnahme einer nationalen Aufsichtsbehörde.

Im Bereich der Polizei und der Justiz dagegen werden die Besonderheiten in den Mitgliedstaaten durch die Regelung allgemeiner Datenschutzgrundsätze in einer Richtlinie weiter gewahrt. Die Richtlinie umfasst als Anwendungsbereich sowohl die Zusammenarbeit von Behörden verschiedener Mitgliedstaaten als auch die Datenverarbeitung innerhalb eines Mitgliedstaates durch Polizei oder Justiz. Sie sieht einheitliche Datenschutzstandards wie z. B. die Unterscheidung zwischen verschiedenen Gruppen von Betroffenen (Zeugen, Verdächtige, verurteilte Straftäter) beim Umgang mit Daten vor und regelt z. B. detailliert das Recht auf Auskunft, Berichtigung und Löschung. Auch enthält die Richtlinie umfassende Rechtsbehelfe für Betroffene, z. B. das Recht auf Beschwerde bei der Datenschutzaufsichtsbehörde.

Reaktionen

Der von der Kommission vorgelegte Entwurf einer Datenschutzreform begegnete sowohl (teilweiser) Zustimmung als auch heftiger Kritik. Insgesamt herrscht in Deutschland vor allem die Sorge, dass man mit den neuen Regelungen hinter dem hier herrschenden hohen Datenschutzstandard zurückbleiben könnte. Begrüßt werden mehrheitlich das grundsätzliche Ziel einer Modernisierung des Datenschutzrechts sowie die beabsichtigte Harmonisierung des Datenschutzrechts in Europa. Auch das „Recht auf Vergessen" sowie die Pflicht zu datenschutzfreundlichen Grundeinstellungen und datenschutzfreundlicher Technologie treffen auf positive Resonanz.
In ihrer ersten Stellungnahme vom 21./22.3.2012 hebt ebenso die Konferenz der Datenschutzbeauftragten des Bundes und der Länder diese positiven Aspekte der geplanten Reform hervor, sieht aber viel Verbesserungsbedarf:

- Gefordert wird die Möglichkeit zur Beibehaltung höherer Schutzstandards insbesondere in Bezug auf besonders sensible Datenverarbeitung.
- Die Grenze von 250 Mitarbeitern hinsichtlich der Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten wird als zu hoch angesehen.
- Die Regelung des „One-Stop-Shop" soll lediglich eine Federführung der Aufsichtsbehörde des Mitgliedstaates der Hauptniederlassung des betreffenden Unternehmens bedeuten, keine ausschließliche Zuständigkeit.
- Das geplante Kohärenzverfahren enthält unscharfe Regelungen.
- Die durch die geplante Grundverordnung begründeten weitreichenden Kompetenzen der EU-Kommission sind problematisch, insbesondere im Hinblick auf die Unabhängigkeit der einzelnen Aufsichtsbehörden.

Am 11.6.12 veröffentlichte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine ausführlichere Stellungnahme mit folgenden Kernpunkten:

- Die in der Verordnung enthaltenen zahlreichen unbestimmten Rechtsbegriffe sowie Interessenabwägungen können zu großen Unsicherheiten in der Praxis führen.
- Ausnahmen für die Datenverarbeitung sollten sich weniger an der Größe eines Unternehmens als an den Gefahren und Risiken für die betroffenen Personen orientieren.
- Es sollen eine Verpflichtung hinsichtlich der Einhaltung technisch-organisatorischer Maßnahmen aufgenommen sowie Regelungen speziell zu Auskunfteien und zum Scoring (wie im BDSG enthalten) ergänzt werden.
  Profilbildung sollte reglementiert werden, insbesondere bei Minderjährigen.
- Die Richtlinie ist in Teilen verbesserungswürdig, bemängelt werden unter anderem die vielen unklaren Regelungen und unbestimmten Rechtsbegriffe.
- Die Möglichkeit der Einschränkung von Betroffenenrechten durch die Mitgliedstaaten wird sehr kritisch gesehen ebenso wie die weit gefassten Ausnahmeregelungen zu Vorschriften zur Übermittlung in Drittländer.
- Auch die Richtlinie sollte die Verpflichtung zur Einhaltung technisch-organisatorischer Maßnahmen enthalten.
- In der Richtlinie sollte klargestellt werden, dass die Mitgliedstaaten über das dort geregelte Mindestmaß hinaus weitergehende Datenschutzregelungen treffen dürfen.

Im Rahmen der durch die geplante Reform entfachten rechtspolitischen Debatten auf allen Ebenen verabschiedete die Konferenz der Datenschutzbeauftragten am 7./8.11.2012 eine weitere Entschließung zu diesem Thema. Die Datenschutzbeauftragten betonen darin vor allem die Unabdingbarkeit des bisher bei jeder Datenverarbeitung geltenden Verbots mit Erlaubnisvorbehalt und lehnen Ausnahmeregelungen für scheinbar weniger schützenswerte Daten ab.
Die Stellungnahme der Art. 29-Gruppe (unabhängiges Beratungsgremium der EU in Datenschutzfragen) vom 25.3.2012 greift unter anderem diese Kritikpunkte auf und enthält Verbesserungsvorschläge insbesondere bezüglich inhaltlicher Klarstellungen. Auch nimmt die Art. 29-Gruppe hierin Stellung zur Richtlinie für den Bereich der Polizei und der Strafjustiz und mahnt die Beibehaltung bisheriger nationaler Standards in diesem Bereich an und fordert hinsichtlich der Grundsätze, Verpflichtungen und Aufgaben, einzelner Rechte und Befugnisse sowie der den Aufsichtsbehörden zur Verfügung stehenden Instrumente eine Vereinheitlichung mit den Regelungen der Grundverordnung.

Ausblick

Der Rat der Europäischen Union und das Europäische Parlament erörtern nun die vorgelegten Entwürfe. Im Parlament befasst sich derzeit der Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres mit den Reformvorschlägen. Der Rat erörtert die Vorlagen in seiner Arbeitsgruppe Datenschutz und Informationsaustausch. Die Länder sind in die Beratungen durch Beteiligung durch die Bundesregierung und durch den Bundesrat eingebunden. Eine Verabschiedung der Reform ist nicht vor 2014/2015 zu erwarten. Die Auswirkungen der europäischen Reform auf das deutsche Datenschutzrecht sind bisher nicht abschließend einzuschätzen, da die vorliegenden Entwürfe aufgrund der starken Kritik sowohl von den nationalen Behörden als auch aus den Reihen der Wirtschaft wohl noch einige Änderungen erfahren werden. Nichtsdestotrotz erscheint mir das mit der Reform verfolgte Ziel der Schaffung eines zeitgemäßen Datenschutzrechts als unbedingt unterstützenswert.

Weitere Informationen: www.bfdi.bund.de

Herausforderung internationaler Datenverkehr: Viele Firmen ahnungslos

Unternehmen übermitteln häufig personenbezogene Daten ins Ausland, z. B. beim Outsourcing von einzelnen Arbeitsschritten an Anbieter im Ausland oder innerhalb von internationalen Konzernen bei zentral geführten Kunden- oder Mitarbeiterdatenbanken. Die besonderen Regeln, die das Bundesdatenschutzgesetz (BDSG) für diese Datenübermittlungen ins außereuropäische Ausland vorsieht, sind vielen Firmen aber nicht bekannt.

Angemessenes Datenschutzniveau

Die Übermittlung personenbezogener Daten an ausländische Stellen unterbleibt, soweit der von der Datenverarbeitung Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den genannten ausländischen Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist (§ 4b Abs. 2 S. 2 BDSG). Dies bedeutet, dass ein Datentransfer grundsätzlich nur in solche Drittländer erfolgen darf, in welchen ein angemessenes (d. h. dem in der EU geltenden vergleichbares) Datenschutzniveau gewährleistet ist. Bei einer Datenübermittlung ins Ausland ist daher jeweils neben der Prüfung der Zulässigkeit der Datenübermittlung an sich (nach den §§ 28–30a BDSG) zusätzlich die Zulässigkeit des Transfers in das Drittland zu prüfen („Zwei-Stufen-Prüfung"). Ist die Datenübermittlung ins Drittland unzulässig, stellt dies sogar eine Ordnungswidrigkeit nach § 43 Abs. 2 Nr. 1 BDSG dar.

Eine Datenübermittlung ins Nicht-EU-Ausland ist nur dann rechtlich zulässig, wenn entweder eine Ausnahmeregelung für die konkrete Datenübermittlung vorliegt oder wenn ein angemessenes Datenschutzniveau im Sinne des § 4 Abs. 2 S. 2 BDSG durch zusätzlich ergriffene Maßnahmen sichergestellt wird.

Eine Datenübermittlung ins Nicht-EU-Ausland ist nur dann zulässig, wenn entweder eine Ausnahmeregelung vorliegt oder ein angemessenes Datenschutzniveau sichergestellt wird.

Verbindliche konzernweite Regelungen (Binding Corporate Rules)

Durch verbindliche Unternehmensregelungen für den internationalen Datenverkehr kann z. B. ein angemessenes Datenschutzniveau im Sinne der EU-Richtlinie erreicht werden (§ 4c Abs. 2 BDSG). Insbesondere bei international tätigen Konzernen mit internem Datenfluss (auch) in Drittländer ist dieses Instrument empfehlenswert. Dabei legt das Unternehmen Regelungen für den Datenschutz beim Transfer von personenbezogenen Daten in diese Drittländer fest. Die Binding Corporate Rules (BCR) müssen einen Schutz bieten, der im Wesentlichen den Kernprinzipien der europäischen Datenschutzrichtlinie entspricht.

BCR unterliegen in Niedersachsen der Genehmigungspflicht der Datenschutzaufsichtsbehörde, welche nach Vorlage der endgültigen BCR einzelne Datenübermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten auf-

grund dieser BCR genehmigt (§ 4c Abs. 2 BDSG). Da die Aufsichtsbehörde die erteilte Genehmigung sowie die BCR dem Bund vorlegen muss und dieser die Genehmigung weiter der EU-Kommission vorlegt, unterliegt die Genehmigung einem Widerrufsvorbehalt (§ 4c Abs. 3 BDSG und Art. 26 Abs. 3 EU-Datenschutzrichtlinie). Zur Vereinfachung des Verfahrens für internationale Konzerne haben sich die Datenschutzaufsichtsbehörden auf ein koordiniertes Genehmigungsverfahren auf europäischer Ebene geeinigt („Mutual Recognition"): Bei internationalen Konzernen mit mehreren Niederlassungen agiert die Aufsichtsbehörde als „Lead Authority", welche den Antrag und den Entwurf der BCR entgegennimmt und bearbeitet, mit dem Antragsteller verhandelt und anschließend den Entwurf den anderen betroffenen Aufsichtsbehörden vorstellt mit der Möglichkeit zur Äußerung. Die Bestätigung der Angemessenheit der BCR gegenüber dem Unternehmen gilt dann für alle Aufsichtsbehörden. Wo dies erforderlich ist (z. B. in Niedersachsen), wird anschließend ohne erneute Prüfung der BCR eine Genehmigung nach § 4c Abs. 2 BDSG von der einzelnen örtlichen Aufsichtsbehörde für ein Mitglied der Unternehmensgruppe erteilt.

Immer mehr Anfragen und Genehmigungsverfahren

Im Berichtszeitraum haben Anfragen und Genehmigungsverfahren zum internationalen Datenverkehr und im Besonderen zu BCR stark zugenommen. In drei Fällen war Niedersachsen federführende „Lead Authority" in Deutschland, in einem Fall wurde bereits eine Genehmigung nach § 4c Abs. 2 BDSG erteilt, in den beiden weiteren läuft das Genehmigungsverfahren noch. Die Anfragen aus diesem Bereich betrafen nicht nur das BCR-Verfahren, sondern auch Fragen der internationalen Auftragsdatenverarbeitung. Leider zeigte sich, dass viele Unternehmen über die besondere Problematik in diesem Bereich keine Kenntnisse haben. Daher stand die Beratung hier im Vordergrund meiner Tätigkeit.

Weitere Informationen:

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

Sanktionen und Rechtsdurchsetzung: Es geht leider nicht ohne

Datensünder müssen bei Verletzung der Datenschutzgesetze mit Konsequenzen rechnen. Den Aufsichtsbehörden in den Bundesländern stehen verschiedene rechtliche Werkzeuge zur Durchsetzung der Datenschutznormen sowie zur Ahndung von datenschutzwidrigem Verhalten zur Verfügung: formelle Anordnungen, Zwangsverfahren und Ordnungswidrigkeitenverfahren.

Zwei Anordnungen

Datenschutzrechtliche Anordnungen können zur Gewährleistung der Einhaltung des Datenschutzrechts gemäß § 38 Abs. 5 Satz 1 Bundesdatenschutzgesetz (BDSG) erlassen werden bei festgestellten Verstößen bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder bei festgestellten technischen oder organisatorischen Mängeln. Bei schwerwiegenden Verstößen oder Mängeln kann die Aufsichtsbehörde gemäß § 38 Abs. 5 Satz 2 BDSG sogar die Datenerhebung, -verarbeitung oder -nutzung untersagen. Dieses Instrument stellt in der aufsichtsbehördlichen Praxis die ultima ratio dar, wenn eine verantwortliche Stelle trotz rechtlicher Hinweise und ausgesprochener formloser Missbilligungen ihr Verhalten dennoch nicht ändert. Die Beratungspraxis zeigt jedoch regelmäßig positive Wirkung, so dass es sehr selten zu formellen Anordnungen kommt. In 2011 habe ich je eine Anordnung wegen unzulässiger Videoüberwachung in einem Bürogebäude sowie wegen der unzulässigen Vervielfältigung von Personalausweisen durch eine Speditionsfirma erlassen (siehe Seite ??).

Acht Zwangsverfahren

Das verwaltungsverfahrensrechtliche Zwangsverfahren kommt dagegen in der Praxis häufiger zur Anwendung. Da meine Aufforderungen zur Auskunft über die Datenverarbeitung bei den Unternehmen leider oft unbeantwortet bleiben, ist eine Durchsetzung meines Rechts auf Auskunft durch Festsetzung eines Zwangsgeldes erforderlich. Weil die vollständige Offenlegung aller Datenverarbeitungen in einem Unternehmen zur Prüfung möglicher Datenschutzverstöße notwendig ist, ist die strenge Anwendung der gesetzlichen Möglichkeiten hier geboten. In den Jahren 2011/2012 habe ich daher in acht Fällen ein Zwangsgeld zur Erlangung einer ausreichenden Auskunft festgesetzt. Als Folge kamen die betroffenen Unternehmen ihrer jeweiligen Auskunftspflicht nach, und auf das Zwangsverfahren folgte dann eine ordnungsgemäße Zusammenarbeit mit der Aufsichtsbehörde.

41 Ordnungswidrigkeitenverfahren

Seit einigen Jahren führe ich zudem verstärkt Ordnungswidrigkeitenverfahren zur Sanktionierung festgestellter Verstöße gegen das Datenschutzrecht durch. Die Art der Verstöße ist dabei gleich geblieben: Am häufigsten wurden auch in 2011/2012 Ordnungswidrigkeitenverfahren wegen Verletzung der Auskunftspflicht gegenüber der Aufsichtsbehörde und gegenüber der betroffenen Person

und wegen unbefugter Datenabfrage bei einer Auskunftei eingeleitet. Daneben gab es mehrere Fälle von Werbung trotz Werbewiderspruchs der betroffenen Person, was ebenfalls mit Ordnungswidrigkeitenverfahren verfolgt wurde. Insgesamt habe ich im Berichtszeitraum 41 Ordnungswidrigkeitenverfahren eingeleitet.

Strafverfahren

In den letzten beiden Jahren habe ich zwei Fälle von Datenschutzverletzungen zur Prüfung einer Strafbarkeit der handelnden Personen an die Staatsanwaltschaft abgegeben. Denn ein Datenschutzverstoß kann auch eine Straftat darstellen, wenn die vorgeworfene Handlung gegen Entgelt oder in der Absicht begangen wurde, sich oder einen anderen zu bereichern oder einen anderen zu schädigen (§ 44 Abs. 1 BDSG). Ich bin hierbei strafantragsberechtigt (§ 44 Abs. 2 BDSG). In dem einen dieser Fälle wurden Mitarbeiter mutmaßlich ohne ihr Wissen von ihrem Arbeitgeber mit Aufzeichnungsgeräten abgehört, im zweiten Fall wurden amtliche Urkunden zu Mitarbeitern von einem Arbeitgeber bei Betriebsauflösung in den Abfall gegeben. In einem weiteren hier bekanntgewordenen Fall hat die Staatsanwaltschaft 2012 tatsächlich Anklage gegen einen Arbeitgeber erhoben wegen strafbarer Datenschutzverletzung, weil er nach Insolvenz seines Unternehmens die Daten seiner Mitarbeiter an ein anderes Unternehmen verkauft hatte. Das Verfahren wurde von der Staatsanwaltschaft gegen Zahlung einer Geldbuße in Höhe von 7.000 Euro abgeschlossen.

AG Sanktionen

Im Jahr 2011 wurde zum besseren Erfahrungsaustausch der Aufsichtsbehörden in diesem Bereich die AG Sanktionen gegründet, die sich mit dem Umgang mit Ordnungswidrigkeiten, Anordnungen und Zwangsmaßnahmen in den Ländern befasst. Die AG hat bisher zweimal jährlich getagt.

Weitere Informationen:

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

3 Technisch-organisatorischer Datenschutz

Cloud-as-cloud-can?
Vom Ringen um datenschutzgerechte Einsatzbedingungen

Das Thema Cloud Computing beherrschte wie kaum ein anderes die Fachpresse und war wiederkehrender Tagesordnungspunkt zahlreicher Veranstaltungen. Dabei lag und liegt die Faszination durchaus nicht nur auf Seiten von IT-Dienstleistern mit Interesse an der Vermarktung neuer Geschäftsmodelle. Während sich die „Cloud" im Consumer-Bereich – insbesondere beim Einsatz von Smartphones und Tablet-Computern sowie als Backup- und Synchronisierungsspeichermedium – immer umfassender realisiert, versprechen sich zunehmend auch IT-Verantwortliche aus Wirtschaft und Verwaltung einen kostengünstigen, einfachen, frei skalierbaren und effizienten Aufbruch zu bisher kaum erreichbaren Ufern. Doch oft werden elementarste Datenschutzanforderungen vernachlässigt.

Cloud Computing bezeichnet nach einer Definition des Bundesamtes für Sicherheit in der Informationstechnik das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software. Bereits in meinem XX. Tätigkeitsbericht (S. 54) habe ich auf das dabei vorherrschende Spannungsfeld zwischen technologischer Machbarkeit und datenschutzrechtlicher Zulässigkeit hingewiesen. Gleichwohl führen unterschiedlichste und teilweise irreführende Begriffsbestimmungen sowie wenig überschaubare Rahmenbedingungen immer wieder zur Vernachlässigung elementarster rechtlicher und technisch-organisatorischer Datenschutzanforderungen.

Bundesamt für Sicherheit in der Informationstechnik: www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html

Datenschutzbeauftragte verabschieden Orientierungshilfe

Konferenz der Datenschutzbeauftragten: www.lfd.niedersachsen.de >Allgemein >DSB-Konferenzen >Entschließungen

Die 82. Konferenz der Datenschutzbeauftragten (DSB) des Bundes und der Länder hat sich bereits im September 2011 der Problematik angenommen und in ihrer Entschließung erste Grundanforderungen an Kontrollierbarkeit, Transparenz und Beeinflussbarkeit Cloud-gestützter Datenverarbeitungen definiert sowie eine Orientierungshilfe „Cloud Computing" der Arbeitskreise Technik und Medien verabschiedet. Darin werden neben zahlreichen Begriffsklärungen und Brückenschlägen zu anderen datenschutzrechtlichen Kernthemen (Auftragsdatenverarbeitung, Rechte der Betroffenen, Mandantenfähigkeit, Schutzziele etc.) insbesondere die zu berücksichtigenden technischen und organisatorischen Aspekte erläutert. Umfassende Darstellung finden die spezifischen Risiken der klassischen Servicemodelle Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) sowie eine Differenzierung der Betriebsmodelle nach dem Aspekt der geografischen Dimension bei den Grundmodellen Public Cloud, Private Cloud und Community Cloud.

Orientierungshilfe Cloud-Computing: www.lfd.niedersachsen.de >Technik und Organisation >Orientierungshilfen >Cloud Computing

Übergreifend werden vier Mindestanforderungen gestellt:

- 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-Anbietern und Cloud-Anwendern;
- Vorlage aktueller Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird zur Gewährleistung der Informationssicherheit und der Portabilität und Interoperabilität durch anerkannte und unabhängige Prüfungsorganisationen.

In der Beratungspraxis begegnete mir zuweilen viel „alter Wein in neuen Schläuchen". Leider gehen bei solchen Umetikettierungen allzu häufig die Hinweise auf die tatsächlichen Inhalte verloren. In so manchem Fall konnte ich nach gründlicher Analyse einem Großteil des Gefährdungspotentials mit wohl erprobten und in der Regel auch bekannten Sicherungsmaßnahmen begegnen.

Fortbildungsangebot für IT-Führungskräfte

Mit einer ganztägigen Fortbildungsveranstaltung zum Thema Cloud Computing hatte ich im Mai 2011 zum inzwischen 13. Expertenkreis für IT-Führungskräfte bei öffentlichen Stellen eingeladen. In dieser Veranstaltung im Rahmen meines Datenschutzinstitutes (DsIN) wurden unter dem Titel „Cloud Computing – endlose Skalierbarkeit zu Lasten des Datenschutzes?" die inzwischen allgegenwärtige Diskussion um diesen Supertrend unter dem Aspekt des wirksamen Grundrechtsschutzes aufgegriffen. Mit fast 30 Teilnehmenden aus den IT-Schlüsselbereichen von Hochschulen, Landesbehörden und Kommunalbehörden war die Obergrenze, die eine Fortbildungsveranstaltung haben sollte, erreicht. Mit einem Symposium hätten zwar mehr Personen angesprochen werden können, der dafür erforderliche organisatorische Rahmen war jedoch aus Kapazitätsgründen nicht leistbar.

Wie immer in dieser Fortbildungsreihe wurde die Veranstaltung von meinem Technikbereich mit einem **Initialreferat zum Telemedienrecht und zum technisch-organisatorischen Datenschutz im Bereich des Cloud Computing** eingeleitet. Dabei wurden zunächst Grundsatzaspekte zum materiellen Recht unter der zentralen Fragestellung „Dürfen sich öffentliche Stellen in der globalen Wolke aufhalten?" beleuchtet. Nach den materiellen Datenschutzbestimmungen bestehen bereits Einschränkungen: Nicht alle Cloud-Modelle ermöglichen den datenschutzkonformen Einsatz. Viele Anbieter auf dem internationalen Markt sind nicht bereit, europäische und deutsche Regelungen umzusetzen. Damit ist eine wirksame Kontrolle durch die verantwortlichen Stellen für die Verarbeitung personenbezogener Daten nicht möglich, und der Einsatz kann demzufolge rechtswidrig sein.

Anhand der typischen Mechanismen von Cloud-Diensten wurden die für personenbezogene Daten relevanten Schutzziele wie Transparenz, Vertraulichkeit, Integrität, Intervenierbarkeit, Nichtverkettbarkeit und Transparenz sowie deren Umsetzbarkeit und deren wirksame Kontrollierbarkeit durch Cloud-Anbieter sowie Auftraggeber und betroffene Privatpersonen differenziert nach den Modellen betrachtet. Die Umsetzbarkeit und Umsetzung von datenschutzrechtlichen Schutzzielen im Cloud-Konzept ist daher je nach Cloud-Modell unterschiedlich. Am ehesten ist unter bestimmten Voraussetzungen in einer Private Cloud ein kontrollierbarer und kontrollierter Einsatz darstellbar. Den Teilnehmern wurden die technischen und organisatorischen Herausforderungen nähergebracht und an den verschiedenen Modellen die Unterschiede aufgezeigt.

Projekt TClouds:
www.tcloudsproject.eu/

Besondere Beachtung wurde auch der gesetzlichen Forderung nach Vorabkontrollen geschenkt. Mit der praktischen Umsetzung von Schutzbedarfsfeststellungen, Schadens- und Risikoanalysen, IT-Sicherheits- und Datenschutzkonzepten, gesetzlich geforderten, angemessenen Schutzmaßnahmen und technischen Implementierungen ging es auch um deren Konkretisierung. Diese Umsetzung muss auf die üblichen Dienstmodelle, getrennt nach den technischen Schichten Infrastructure as a Service (IaaS), Platform as a Service (PaaS) und Software as a Service (SaaS) erfolgen. Außerdem muss nach den Betriebsmodellen (Private Cloud, Public Cloud, Community Clouds und Hybrid Cloud) unterschieden werden, die aus Datenschutzsicht differenziert zu bewerten sind. Zentrale Anforderung ist dabei, dass in der je-

weiligen Variante der Dienstmodelle, getrennt nach den technischen Schichten, die datenschutzrechtlichen Anforderungen für die verantwortliche Stelle jeweils einzeln festlegbar und beherrschbar sind. Schließlich wurden Anforderungen beleuchtet, die an die denkbaren Vertragsmodelle und Service Level Agreements (SLA) für die Datenverarbeitung im Auftrag gestellt werden müssen.

Mit weiteren Beiträgen wurden in der Expertenveranstaltung verschiedene Cloud-Projekte aus der Praxis vorgestellt und mit dem Fachteilnehmerkreis diskutiert. Mit dem Vortrag **„Trustworthy Cloud Computing – Konzept und Bedingungen für vertrauenswürdiges Cloud Computing"** präsentierten Referenten vom Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) konkrete Ergebnisse einer Studie zu den Bedingungen, die an ein datenschutzrechtlich vertrauenswürdiges Cloud-Konzept zu stellen sind. Hier konnte auch auf Erfahrungen im Projekt „TClouds" (Trustworthy Clouds Privacy and Resilience for Internet-scale Critical Infrastructure) zurückgegriffen werden, an dem das ULD maßgeblich beteiligt ist. Dies ist ein von der Europäischen Kommission gefördertes internationales Projekt mit 14 Partnern aus ganz Europa, an dem das ULD beteiligt ist, und das noch bis September 2013 läuft. Ziel des Projektes ist die Schaffung einer Cloud-Umgebung, die den europäischen Sicherheits- und Datenschutzanforderungen gerecht wird. Die Umsetzung soll an zwei konkreten Anwendungsszenarien erfolgen: ein Smart Grid zur Verwaltung der öffentlichen Straßenbeleuchtung in Portugal und ein eHealth-Verfahren in Italien. Mit diesem Beitrag wurden in der Veranstaltung insbesondere die rechtlichen Anforderungen, die Steuerung der Verarbeitungsprozesse und die tatsächliche Durchsetzbarkeit von Schutzmaßnahmen betont, die eine Auftragsdatenverarbeitung nach § 11 Bundesdatenschutzgesetz (BDSG) bzw. § 6 Niedersächsisches Datenschutzgesetz (NDSG) innerhalb Deutschlands oder der EU-Mitgliedsländern betrifft. Das Ergebnis des Projektes soll als Open-Source-Lösung verfügbar gemacht werden.

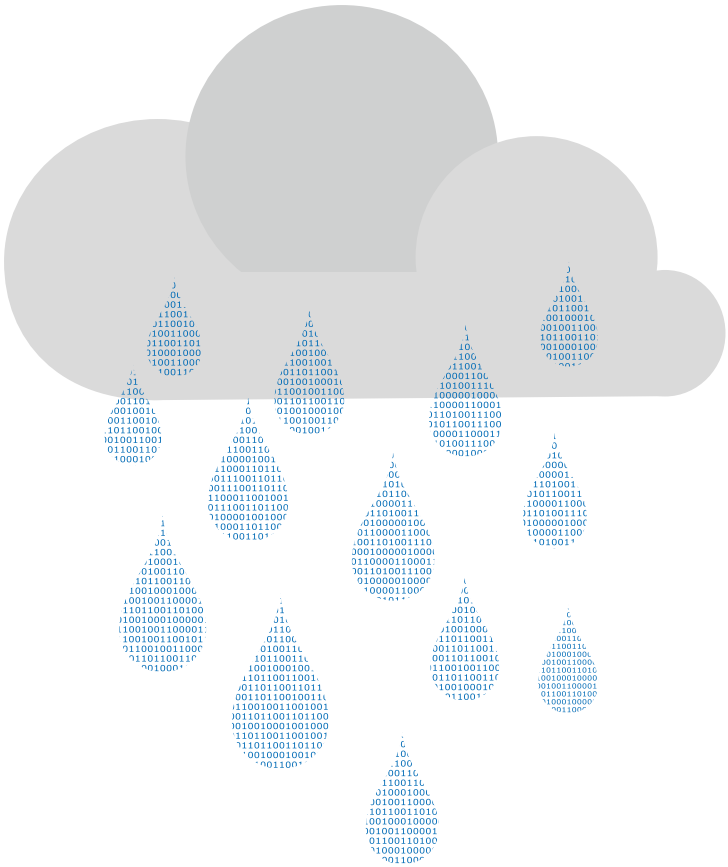
Forschung Netz- und Datensicherheit: www.nds.ruhruni-bochum.de/chair/people/dominik-birk/

Es mangelt an Verfügbarkeit, Integrität und Vertraulichkeit

Eine ebenfalls zentrale Herausforderung stellt die Informationssicherheit einschließlich der IT-Sicherheit im engeren Sinne dar. „Cloud Computing Security" stellt zum technisch-organisatorischen Datenschutz zum einen ein Pendant dar, und ihre Ziele weichen durch das Datenschutzziel der Datensparsamkeit voneinander ab. Zum anderen stellen IT-Security-Maßnahmen und technischer Datenschutz oftmals Überschneidungen dar und ergänzen sich auch gegenseitig. Aus Sicht der Forschung referierte hierzu ein Wissenschaftlicher Mitarbeiter beim Lehrstuhl für Netz- und Datensicherheit von Prof. Dr. Jörg Schwenk des Horst Görtz Institute for IT-Security an der Ruhr-Universität Bochum (http://www.nds.ruhruni-bochum.de/chair/people/dominik-birk/) die Erkenntnisse und Forschungsaktivitäten mit dem Titel **„Cloud Computing Security"**. Hier wurden nicht nur forensische Ansätze der verschiedenen Risiken präsentiert, sondern auch die globalen Unterschiede der Datenschutz- und IT-Sicherheitsniveaus aufgrund der jeweiligen Netzpolitik der Länder aufgezeigt. Daraus lässt sich ableiten, dass aufgrund der faktischen Unkenntnis des Endkunden über den Speicherort der Daten in der Cloud keineswegs von einer verlässlichen

Projekt OPTIMIS: www.iri.uni-hannover.de/optimis-1635.html

www.optimis-project.eu/project



Verfügbarkeit, Integrität und Vertraulichkeit ausgegangen werden kann. Als eines der Hauptprobleme stellt sich auch der überwiegende Verzicht der Dienstleister auf Verschlüsselung der Datenspeicher (Datenbanken und File-Systemen der Cloud-Provider) und der Kommunikation (z. B. sichere Übertragung mittels SSL/TLS-Verschlüsselung) mit den Servern dar. Zahlreiche Anbieter überlassen es durch Nutzungsbedingungen den Kunden, für den notwendigen Schutz durch Verschlüsselung zu sorgen. Zudem halten Global-Public-Cloud-Anbieter ihre Strukturen und teilweise auch die Standorte der Rechenzentren aus Wettbewerbs- und Sicherheitsgründen geheim. Das dient zwar vordergründig der IT-Sicherheit, verhindert jedoch die Transparenz und die notwendigen Kontrollen und Reviews seitens der Kunden. Somit verlassen sich Kunden ausschließlich auf die unzureichende Kenngröße des Vertrauens. Dieses Vertrauen ist angesichts der vorgenannten internationalen Unterschiede bei den Netzpolitiken, bei dem sehr unterschiedlichen Potential der Internetkriminalität und bei den höchst differenzierten datenschutzrechtlichen Rahmenbedingungen jedoch keinesfalls gerechtfertigt.

Ein wissenschaftlicher Vertreter des Instituts für Rechtsinformatik (IRI) der Gottfried Wilhelm Leibniz Universität Hannover, Lehrstuhl von Prof. Dr. Nikolaus Forgó, stellte das bis Mai 2013 befristete **Konsortial-Projekt „OPTIMIS"** vor. Ziel dieses Projektes ist es, ein offenes und verlässliches „Cloud-Service-Ecosystem" auf der Basis einer Hybrid-Cloud zu entwickeln, das IT-Services bietet, die anpassungsfähig, zuverlässig, nachvollziehbar und nachhaltig (ökologisch und ökonomisch) sind. Organisationen sollen damit automatisch und nahtlos externalisierte Dienste und Anwendungen von vertrauenswürdigen und nachvollziehbaren Cloud-Anbietern beziehen können.

http://www.iri.uni-hannover.de/optimis-1635.html und http://www.optimis-project.eu/project

Um ein konkretes Beispiel eines Projektes der Landesverwaltung aufzugreifen, präsentierte der Referent für Informationsmanagement des Niedersächsischen Ministeriums für Wissenschaft und Kultur mit dem Titel „Wie viel ‚kostenlos' wollen können wir uns leisten?" die **Cloud-Strategie für die niedersächsischen Hochschulen**". In dem Projekt „NDS Storage Cloud" wird in einer ersten Ausbaustufe das Ziel verfolgt, im Verbund der niedersächsischen Hochschulen die Nutzung der Storage-Kapazitäten in einer Private-Cloud-Struktur zu optimieren. Die Installation und der Betrieb von Speicher im Verbund mit niedersächsischen Hochschulen begannen 2011 mit der Beschaffung und der Inbetriebnahme. Die Kontrolle verbleibt hier vollständig in der Hand der öffentlich-rechtlichen Hochschulen mittels eines Storage Management Services.

Kein ordnungsgemäßer Betrieb mit Public-Cloud-Angeboten

Die während und nach den Fachvorträgen geführten Diskussionen warfen nicht nur zahlreiche Fragen auf. Sie lieferten auch Erkenntnisse zur Frage der Zulässigkeit und Ausgestaltung der verschiedenen Betriebsmodelle und IT-Strategien sowie der nach dem geltenden Recht geforderten angemessenen technisch-organisatorischen Schutzmaßnahmen vor dem Hintergrund des technisch Machbaren sowie der tatsächlichen wirtschaftlichen Realitäten beim Cloud Computing. Ein Ergebnis war, dass Public-Cloud-Angebote für einen ordnungsgemäßen Betrieb aus datenschutzrechtlicher Sicht nicht in Frage kommen, während Private-Cloud-Angebote bei entsprechenden vertraglichen Kontrolloptionen seitens des Kunden Lösungsoptionen bieten.
Über die Ergebnisse der Veranstaltung wurde auch die Arbeitsgruppe (AG) „Cloud Computing" des Arbeitskreises „Technische und organisatorische Datenschutzfragen" der Datenschutzbeauftragten des Bundes und der Länder informiert, deren Federführung beim Hessischen Datenschutzbeauftragten lag. Diese AG hatte die Orientierungshilfe erarbeitet. Gewichtige rechtliche Fragen bleiben im Fazit aber weiterhin bestehen. So steht die Evaluierung und Modernisierung des europäischen und deutschen Datenschutzrechts aus. Im Fall von außereuropäischen Cloud-Anbietern stellt sich die Frage nach der Sinnhaftigkeit und Zukunft des Safe-Harbor-Status. Derzeit mehrt sich auch die Kritik innerhalb der US-Aufsichtsbehörde. In Europa ist am Ende des Berichtszeitraumes noch offen, ob, wann und wie eine Evaluierung des Abkommens durch die EU erfolgen wird. Jedenfalls ist derzeit die grenzüberschreitende Datenverarbeitung mit Ländern außerhalb der EU bzw. der Freihandelszone des Europäischen Wirtschaftraumes (EWR) mit den Vorgaben des deutschen und europäischen Datenschutzrechts höchst unsicher und offensichtlich nicht vereinbar.

Outsourcing des Desktopmanagements: Land nimmt schleichenden Kontrollverlust in Kauf

Am 14.12.2010 beschloss die Landesregierung, das Desktopmanagement (DTM; zentrale Verwaltung und Steuerung der IT-Infrastruktur am Arbeitsplatz) für rund 7.500 Arbeitsplätze der Landesverwaltung an einen externen Dienstleister zu übertragen. Vorausgegangen war eine knapp einjährige vom Niedersächsischen Ministerium für Inneres und Sport durchgeführte Vorbereitungsphase. Unter Beteiligung aller Ressorts wurden die Rahmenbedingungen analysiert und eine mit Hilfe externer Beratung erstellte Wirtschaftlichkeitsbetrachtung zu Grunde gelegt. Aber auch dieses Outsourcing-Projekt greift in Kernbereiche des Datenschutzes ein.

Als wenig konstruktiv erschien durch dieses Vorhaben die Situation, in die der Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) manövriert wurde. Der Landesbetrieb hatte als zentraler IT-Dienstleister des Landes bisher diese Aufgabe wahrgenommen und war jetzt im Begriff, durch sehr aufwändige Zuarbeiten die ohnehin angespannte Arbeitssituation bis an die Grenzen belasten zu müssen und letztendlich doch noch einen weiteren Grundpfeiler des eigenen Aufgabenbereiches zu verlieren.

„Hase und Igel" mal anders …

Zum wiederholten Male trat auch an dieser Stelle ein Automatismus in Erscheinung, auf dessen Gefahrenpotential ich schon mehrfach hingewiesen habe, unter anderem in meinem XX. Tätigkeitsbericht 2009–2010, S. 102 ff. Der seit 2005 durch diverse Verwaltungsmodernisierungsmaßnahmen betroffene LSKN, dem nie die Möglichkeit zu einer ausreichend schnellen und flexiblen Anpassung des Personalbestandes an steigende Anforderungen eingeräumt worden war, verlor zwangsläufig einen weiteren Wettlauf im Rahmen des „Outsourcing-Cups" der Landesregierung. Die Risiken, die auch hier mit der Vergabe nicht-hoheitlicher, allerdings sehr wohl existentieller infrastruktureller Kernaufgaben eingegangen werden sollten, sind meines Erachtens nicht hinreichend gewürdigt worden. Der Abbau landeseigener Kompetenzen, die erhöhte Komplexität vertraglich zu regelnder Leistungsgeflechte und ein damit einhergehender schleichender Kontrollverlust gefährden nicht nur die optimale Ausgestaltung des rein operativen Geschäfts, sie erschweren zumindest tendenziell auch die gesetzlich geforderten Datenschutzkontrollmöglichkeiten.
Dies habe ich auch in den mit dieser Thematik befassten Sitzungen des Niedersächsischen IT-Planungsrates hervorgehoben. Ich hatte im Rahmen des Auftaktworkshops „Leistungsverzeichnis" im Frühjahr 2011 Gelegenheit zur ausführlichen Darlegung datenschutzrechtlicher Anforderungen. Neben der Benennung rechtlicher Erfordernisse konnte ich zahlreiche Anmerkungen und Fragestellungen zum vorgelegten Entwurf des Leistungsverzeichnisses einbringen. Insbesondere habe ich eindringlich auf die mögliche „Hilflosigkeit" der betroffenen Dienststellen angesichts eigener datenschutzrechtlicher Verantwortung, der Zuständigkeiten des LSKN, der Zuständigkeiten beauftragter Subunternehmer und möglicherweise zwischengeschalteter Provider-Manager hingewiesen. Die Sitzungen des zur weitergehenden Abstimmung mit den Ressorts eingerichteten sogenannten IT-Boards habe ich informell begleitet und

zuletzt zur Bestimmung des Schutzbedarfes der personenbezogenen Daten Stellung genommen.
Das ebenfalls mit externer Beratung vorbereitete und durchgeführte DTM-Vergabeverfahren wurde im Juni 2011 gestartet und im September 2012 mit der Zuschlagserteilung an die Fa. T-Systems beendet. Die Vereinbarung beinhaltet eine Erweiterungsoption, die eine Ausweitung der Dienstleistung auf weitere 33.000 Arbeitsplätze ermöglicht.

… denn am Schluss kommt womöglich keiner ins Ziel

Kurz nach der Erfolgsmeldung der Landesregierung, das komplexe Procedere erfolgreich abgeschlossen zu haben, musste an anderer Stelle ein deutlicher Rückschlag konstatiert werden: Am 18.12.2012 gab das Innenministerium offiziell eine im gegenseitigen Einvernehmen erfolgte umfangreiche Reduzierung des Rahmenvertrages TK2010 bekannt. War beim Start des Umsetzungsprojektes „Niedersachsen Next-Generation-Network“ (NI-NGN) im März 2009 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, sah man sich nunmehr gezwungen, in wesentlichen Teilen Abstriche zu machen. Insbesondere die Leistungserbringung in den Bereichen „Lokale Netze“ und „Sprachkommunikation“ wurde annulliert und die Migration weiterer Standorte ausgesetzt. Es bleibt abzuwarten, welchen Fortgang dieses konkrete Vorhaben nimmt und welche Konsequenzen zur Vermeidung ähnlicher Fehleinschätzungen in anderen Projekten gezogen werden.

Und was hat das mit Datenschutz zu tun?

Dass in diesen und ähnlichen von Technik geprägten sogenannten „horizontalen Querschnittsaufgaben“ personenbezogene Daten verarbeitet werden, ist unbestritten. Ein Blick auf die „Elementaren Datenschutzziele“ (siehe Seite 100) macht deutlich, wie tief Outsourcing-Projekte in alle diese Kernbereiche eingreifen. Gleiches lässt sich aus den mit § 7 Abs. 2 NDSG geforderten Datenschutzkontrollen ableiten.
Um dies rechtzeitig erkennen, sicher einschätzen und auf Dauer verantwortungsvoll handhaben zu können, ist es wichtig,

- eindeutige und transparente Regelungen nicht nur für die Wahrnehmung datenschutzrechtlicher Überlegungen zu schaffen,
- ein höheres Maß an Kontinuität bei der Ressourcenplanung anzustreben
- und insbesondere die landeseigene Kompetenz zu stärken und zukunftsfähig aufzustellen.

Es bleibt zu hoffen, dass der gebeutelte „Hase“ LSKN nicht zu häufig fallengelassene Staffelstäbe wieder aufnehmen und letztendlich das ungleiche Rennen mit seinen alten Turnschuhen fortsetzen muss.

Neues Internetprotokoll IPv6: Beobachtung und Identifizierung problemlos möglich

Das Internetprotokoll (IP) ist heute der am weitesten verbreitete Protokollstandard zur Übermittlung von Daten in Rechnernetzen, insbesondere im Internet. Die noch weit verbreitete Version 4 (IPv4) wurde bereits 1981(!) definiert und ermöglicht aufgrund der Adresslänge von 32 Bit die Adressierung von maximal 4.294.967.296 (2^{32}) Teilnehmeranschlüssen. Da dieser Adressbereich bereits in der Vergangenheit nicht mehr ausreichend war, wurde mit technischen Tricks wie zum Beispiel der dynamischen Adressvergabe und der Umsetzung mehrerer privater Netzwerkadressen auf eine öffentliche Adresse (NAT) gearbeitet, um den Bedarf abzudecken. Diese Tricks haben zwar den technischen Aufwand erhöht, boten aber gleichzeitig eine datenschutzrechtlich zu begrüßende Zwangspseudonymisierung für sehr viele private Netzteilnehmer.

Nachdem weltweit die letzten freien IPv4-Adressen vergeben sind, lässt sich die technisch längst überfällige Einführung des immerhin schon 1998 definierten Nachfolgers IPv6 nicht mehr länger hinauszögern. Dieser „neue" Standard löst das Problem der Adressknappheit durch die Verwendung von 128-Bit langen, also viermal längeren Adressen. Dadurch steigt der Adressvorrat in astronomische Größenordnungen (2^{128}), und erlaubt die Vergabe von statischen Adressen an eine nahezu beliebige Anzahl von Netzteilnehmern und jedwede Art von technischen Systemen. Auf diese Weise wäre auch der Weg frei für die weltweit eindeutige Identifizierung aller Arten von Kleinstendgeräten – vom Haushaltsgerät, über Preisschilder im Einzelhandel bis zu sämtlichen mobilen und stationären IT-Endgeräten. Damit soll – nach dem Wunsch von Industrie und Handel – schließlich das „Internet der Dinge" Realität werden.

Orientierungshilfe der Datenschutzbeauftragten

Durch diese erweiterten Möglichkeiten zur Vergabe statischer Adressen entfällt die Notwendigkeit der technischen Tricks zur Mehrfachnutzung von IP-Adressen. Daraus ergeben sich auch datenschutzrechtliche Folgen: Jeder Netzteilnehmer könnte an Hand seiner dauerhaft vergebenen statischen Adressen bei allen Netzaktivitäten problemlos beobachtet und identifiziert werden. Dies wäre für die meisten Privatanwender und eine Reihe von mittelständischen Unternehmen eine erhebliche Verschlechterung der derzeitigen Datenschutzsituation. Andererseits eröffnet eine statische Adressvergabe aber auch erheblich verbesserte Möglichkeiten, personenbezogene Daten bei der Veröffentlichung im Internet innerhalb des eigenen, selbst

kontrollierten Bereichs zu belassen und somit einem Missbrauch wirkungsvoll entgegenzutreten.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat daher 2011 und 2012 in zwei Entschließungen alle Beteiligten zur Wahrung und Verbesserung des bestehenden Standards zum Datenschutz und zur IT-Sicherheit bei der Umstellung auf IPv6 aufgefordert. Anbieter von Internetzugängen und Diensten sowie Hersteller von Hard- und Software-Lösungen sollten ihre Produkte datenschutzgerecht gestalten (privacy by design) und dementsprechende Voreinstellungen wählen (privacy by default). Internetnutzenden wird darin empfohlen, bei der Beschaffung von Hard- und Software sowie beim Abschluss von Verträgen auf diese Aspekte besonders zu achten.
Als unterstützende Maßnahme, insbesondere für Provider mit Endkundenbeziehung sowie Hersteller von Geräten für Privatkunden, verwiesen die Datenschutzbeauftragten in der zweiten Entschließung auf eine im Oktober 2012 fertiggestellte Orientierungshilfe „Datenschutz bei IPv6 – Hinweise für Hersteller und Provider im Privatkundengeschäft“. Damit soll bei der Umsetzung dieser Forderungen die Beachtung und Verbesserung der bestehenden Datenschutzstandards erleichtert werden.

Weitere Informationen:

Entschließungen und Orientierungshilfe:
www.lfd.niedersachsen.de/
Technik und Organisation/Orientierungshilfen und Handlungsempfehlungen

Dienstliche Nutzung privater Mobilgeräte: Unverschlüsselte Schülerdaten auf Lehrer-Smartphones

Im Zuge des Neuentwurfs eines Erlasses des Kultusministeriums zur Verarbeitung personenbezogener Daten auf privaten Systemen von Lehrkräften konnte ich zwar verschiedene Verbesserungen im Vergleich zum alten Erlass erreichen. So erstreckt sich die Regelung nun nicht mehr nur auf klassische Datenverarbeitung an PC oder Notebooks, sondern bezieht auch die inzwischen sehr verbreiteten mobilen Geräte wie Smartphones oder Tablet-PCs mit ein. Eine generelle Vorgabe zur Verschlüsselung gibt es jedoch nach wie vor nicht.

Darüber hinaus wurde ein enger Datenrahmen gesetzt, der ausschließlich die Verarbeitung von einzelnen Schülerdaten erlaubt; eine weitergehende Verwendung von Eltern- oder Lehrerdaten auf privaten Systemen ist hingegen ausgeschlossen. Des weiteren wurde zur partiellen Stärkung des Datenschutzes durch die klare Vorgabe beigetragen, Daten bei Übertragung über öffentliche Medien oder Transport mit Hilfe von Datenträgern wie USB-Sticks oder -Festplatten angemessen zu verschlüsseln; gleiches gilt bei externer Speicherung in sogenannten Cloud-Diensten.

Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen von Lehrkräften: Erlass des Kultusministeriums unter www.lfd.niedersachsen.de >Themen >Schulen

Eine generelle Vorgabe zur Verschlüsselung, auch auf den jeweiligen privaten Rechnern, ist leider nicht erfolgt. Gerade bei der Ablage und Nutzung der Daten auf Smartphones, die ebenso leicht verloren gehen können wie USB-Sticks, sind dies nach meiner Auffassung unzureichende Vorgaben. Entsprechende Hinweise meinerseits für die Ausgestaltung des neuen Erlasses wurden jedoch leider nicht berücksichtigt.

Eine nach meiner Ansicht erforderliche vollständige Abkehr von dem Weg, die Nutzung privater Endgeräte zu erlauben, ließ sich bedauerlicherweise bisher nicht erreichen. Zudem gelten die marktüblichen Betriebssysteme mit ihren Apps auf mobilen Endgeräten (Android, iOS usw.) als prinzipiell unsichere Plattformen, weil sie in oftmals intransparenter und überbordender Weise Nutzerdaten über das Mobilfunknetz senden und zu wenige, unvollständige oder schlecht bedienbare Datenschutzkonfigurationsoptionen bieten. Den öffentlichen Stellen obliegt als Daten verarbeitende Stelle (im Sinne des § 3 Abs. 3 NDSG) die Verantwortung für die technisch und organisatorisch erforderlichen Maßnahmen im Sinne des § 7 NDSG. Werden personenbezogene Daten jedoch auf privaten Endgeräten verarbeitet, entzieht sich der Prozess faktisch dem Einflussbereich der verantwortlichen Administration. Schutzmaßnahmen können auf diese Weise nicht mehr organisiert und wirksam durchgesetzt und kontrolliert werden. Die Lehrkraft wird mit dem verantwortlichen und fachkundigen Umgang der technischen und organisatorischen Datenschutzmaßnahmen faktisch allein gelassen und damit überfordert.

Meines Erachtens lässt sich dieses Grundproblem nur nachhaltig lösen, wenn Lehrkräfte ausschließlich dienstliche Geräte mit gehärteten Betriebssystemen und getesteten und freigegebener Anwendungssoftware (Apps) unter zentraler Administration nutzen könnten. Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten von Bund und Ländern hat 2012 beschlossen, eine Orientierungshilfe zum Thema private Endgeräte im beruflichen/dienstlichen Umfeld („Bring Your Own Device“) zu entwickeln. Der Trend, dass immer mehr private Endgeräte und privat organisierte Cloud-basierte Speicher- und Verarbeitungsressourcen genutzt werden, ist seit einiger Zeit erkennbar. Oft wird auf eine kontrollierte Administration (etwa durch ein Device-Management) vor allem aus eigentumsrechtlichen Gründen verzichtet. Der daraus resultierende Kontrollverlust, die damit einhergehenden Risiken für die Informationssicherheit und den Datenschutz sowie die teilweise in Kauf genommenen Rechtsverstöße stellen die verantwortlichen datenverarbeitenden Stellen vor große Schwierigkeiten.

Drahtlosnetzwerke an Schulen: Verschlüsselung ist Pflicht

Immer wieder erreichen mich Anfragen zur Nutzung von WLAN (Wire-less Local Area Network; lokales Funknetz) an Schulen. Die aufgeworfenen Fragen reichen dabei von technischen Details der Zugangs- und Übertragungssicherheit bis hin zu Fragen zum Telekommunikations- und Telemedienrecht.

Generell ist zu beachten, dass ein WLAN nicht nur an Schulen gegen unbefugte Nutzung abzusichern ist. Dies geschieht zweckmäßigerweise durch eine Kombination aus aktueller Verschlüsselung nach WPA2 und weiteren Konfigurationsmaßnahmen wie Geräteadress-Filterung und Netzabschaltung außerhalb der normalen Nutzungszeiten. Dabei ist die Nutzung des WLAN stets auf dienstliche Geräte zu beschränken. Wird dies unterlassen, könnte das WLAN auch für Dritte nutzbar sein und sich die Schule möglicherweise in der Rolle eines Telekommunikations-Diensteanbieters wiederfinden. Darüber hinaus besteht bei einer Nutzung durch Dritte stets die Verantwortlichkeit als Anschlussinhaber für heruntergeladene Inhalte aus dem Internet. In Bezug auf das WLAN für Sicherheit zu sorgen, ist daher eine wesentliche Verpflichtung der Schulleitung, die stellvertretend für die Schule die volle Verantwortung für jegliche Art von Missbrauch trägt.

Ebenfalls bei der Schulleitung liegt die Verantwortung für Angebote einer Schul-Homepage; wichtig ist in diesem Zusammenhang die Beachtung der Informationspflichten (Impressum) nach den Bestimmungen des Rundfunkstaatsvertrages und des Telemediengesetzes.

WPA2 (Wi-Fi Protected Access 2) ist ein technischer Sicherheitsstandard, der mit einer AES-Verschlüsselung (Advanced Encryption Standard) arbeitet.

Weitere Informationen:

Orientierungshilfe Datenschutz in drahtlosen Netzen:
www.lfd.niedersachsen.de
>Technik und Organisation >Orientierungshilfen und Handlungsempfehlungen

Schutzziele statt Kontrollziele: Neues Referenzmodell für technische und organisatorische Datenschutzmaßnahmen

Bereits im letzten Berichtszeitraum (2009–2010) nahm das Thema der Modernisierung der datenschutzrechtlichen Schutzziele eine wichtige Stelle für den technisch-organisatorischen Datenschutz ein. Eine der Grundlagen des Eckpunktepapiers der Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahre 2010[1] war die schon länger bestehende Erkenntnis, dass dem Ansatz „privacy by design", also der Integration technischer Datenschutzmaßnahmen bereits in die Konstruktion von Hardware und in die Implementierung der Software von IT-Systemen, wirksamer gefolgt werden müsste. Dazu sollten die bisherigen Kontrollziele durch die Definition eines Systems abschließender elementarer Schutzziele[2] ersetzt werden, die systematisch aufeinander bezogen sind und universell gelten sollen.

Rechtlich ist derzeit in Niedersachsen das System der Schutzmaßnahmen für öffentliche Stellen in § 7 NDSG durch so genannte Kontrollziele definiert. Es sind dies

- Zugangskontrolle,
- Datenträgerkontrolle,
- Speicherkontrolle,
- Benutzerkontrolle,
- Zugriffskontrolle,
- Übermittlungskontrolle,
- Eingabekontrolle,
- Verfügbarkeitskontrolle,
- Auftragskontrolle,
- Transportkontrolle und
- Organisationskontrolle.

Im nicht-öffentlichen Bereich entspricht diese Regelung der des § 9 BDSG mit der dazugehörigen Anlage.
Das System neuer elementarer Schutzziele ist inhaltlich bereits in Teilen bekannt. Auch die Europäische Datenschutzrichtlinie kennt Verfügbarkeit, Integrität, Vertraulichkeit und Prüfbarkeit. Das Bundesverfassungsgericht stattete 2008 zwei dieser Ziele mit Verfassungsrang aus und entschied, dass das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG[3]) auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. Inzwischen hat beispielsweise der Landesgesetzgeber in Schleswig-Holstein alle sechs elementaren Schutzziele übernommen. Danach ist

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

2 Vgl. Aufsatz Rost, Martin / Pfitzmann, Andreas, 2009: Datenschutz-Schutzziele – revisited; in: DuD – Datenschutz und Datensicherheit, 33. Jahrgang, Heft 6, Juli 2009: 353–358

3 Bundesverfassungsgericht: BVerfG, 1 BvR 370/07 vom 27.2.2008: www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

die Ausführung der Datenschutzvorschriften durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Diese Maßnahmen müssen gewährleisten, dass

1. Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (Verfügbarkeit),
2. Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (Integrität),
3. nur befugt auf Verfahren und Daten zugegriffen werden kann (Vertraulichkeit),
4. die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (Transparenz),
5. personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (Nicht-Verkettbarkeit) und
6. Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte (insbesondere §§ 16, 17 Abs. 3, 17a, 19 und 20 NDSG sowie §§ 6, 19, 20, 21, 28 Abs. 4, 34 BDSG) wirksam ermöglichen (Intervenierbarkeit).

Eine solche Gesetzesnovellierung hat nach meiner Auffassung für andere Länder – so auch für Niedersachsen – Vorbildcharakter, weil sie sich besser der stark geänderten Welt unserer Informations- und Internetgesellschaft mit der zunehmenden Mobilisierung allgegenwärtiger IT-Systeme anpassen ließe. Diese sechs neuen elementaren Schutzziele wurden von einer Unterarbeitsgruppe des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder im Hinblick auf die spezifischen Anforderungen des Datenschutzes entwickelt.

Standardisiertes Datenschutzmodell stellt Personen in den Mittelpunkt

In der Fortentwicklung des Themas auf der Grundlage des vorgenannten „Eckpunktepapiers 2010“ setzte sich die Erkenntnis durch, dass über die reine Schutzzieledefinition hinaus deren Einbettung in der täglichen Praxis erforderlich ist. Um dies praxistauglich zu schaffen, bedurfte es einer weiteren Erarbeitung einer Standardisierung. Dazu entwickelte federführend das Unabhängige Datenschutzzentrum Schleswig-Holstein (ULD)[4] unter Mitarbeit mehrerer Technikbereiche der Landesdatenschutzbeauftragten ein so genanntes Standardisiertes Datenschutzmodell (SDM). Es stellt im Ergebnis einen Ansatz in Anlehnung an die Grundschutz-Methodik dar und wurde im Oktober 2012 mit einem Zwischenbericht dem Arbeitskreis Technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorgestellt. Trotz Anlehnung liegt der Unterschied zur Grundschutzdefinition[5] des Bundesamts für Sicherheit in der Informationstechnik (BSI) jedoch darin, dass nicht die Geschäftsprozesse einer Organisation im Mittelpunkt stehen müssen, sondern die Perspektive der betroffenen Personen einzunehmen

4 Vgl. Martin Rost, Kirsten Bock: Privacy By Design und die Neuen Schutzziele; Grundsätze, Ziele und Anforderungen; in DuD • Datenschutz und Datensicherheit Heft 1/2011

5 BSI-Standard 100-2 IT-Grundschutzvorgehensweise https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf

ist, denn Datenschutz als Grundrechtsschutz hat nicht den Schutz einer Organisation im Blick, sondern primär den von Personen.

Als Schutzbedarfskategorien gelten die Stufen
- normal,
- hoch und
- sehr hoch.

Das SDM betrachtet zudem ein Verfahren mitsamt seinen typischen drei Komponenten:
- Daten und ihre Datenformate,
- IT-Systeme und Schnittstellen,
- Prozesse und adressierbare Rollen.

Referenzmodell ohne zusätzlichen Lernaufwand für Behörden und Betriebe

In der kombinierten Betrachtung der sechs elementaren Schutzziele mit den drei Schutzbedarfskategorien und den drei Verfahrenskomponenten ergibt sich im SDM also multipliziert ein Satz aus 54 zu definierenden Datenschutzmaßnahmen. Dieses dadurch entstandene Referenzmodell ist geeignet, als Prüfmuster für jedes IT-Verfahren zugrunde gelegt zu werden. Und es kann durch Anpassbarkeit als generisch und skalierbar gelten. Die Vorteile dieses SDM liegen zum einen in der Passgenauigkeit bezüglich der gesetzlichen Datenschutzziele und zum anderen darin, dass die strukturelle Ähnlichkeit mit der Vorgehensweise im Informationssicherheitsmanagement keinen eigenständigen neuen oder zusätzlichen Lernaufwand bei behördlichen und betrieblichen Datenschutzbeauftragten oder Auditoren verursacht. Gleichwohl wird die Möglichkeit eröffnet, methodisch ähnlich und parallel vorzugehen, um technische und organisatorische Maßnahmen der Informationssicherheit mit denen des Datenschutzmodells zeitnah abzugleichen. Synergieeffekte im Alltag der Entwicklung und Anpassung von IT-Systemen sind damit also ebenfalls nutzbar.
Mit Beginn des Jahres 2013 hat die Arbeitsgruppe des AK Technik begonnen, an einer Weiterentwicklung und einer Verfeinerung des SDM zu arbeiten. Wünschenswert wäre aus meiner Sicht eine konsequente Einarbeitung des Modells in den Entwurf der derzeit auf dem Weg befindlichen europäischen Datenschutzgrundverordnung, aber auch in die Ländergesetze. Aufgrund der Globalisierung der IT, besonders in den Bereichen von Cloud-Diensten, IT-Hard- und Softwareprodukt-Verbreitung und Social-Media-Plattformen, ist zudem eine verstärkte Befassung mit diesem Ansatz auf internationaler Ebene und in Normungsgremien erforderlich, um zu systematischeren Vorgehensweisen zu gelangen und diesem Modernisierungsvorhaben den erforderlichen öffentlichen Bekanntheitsgrad in der Fachwelt und schließlich in der Gesellschaft zu verleihen. Ich bin davon überzeugt, dass dem Grundrechtsschutz damit insgesamt gedient wäre.

Mandantenfähigkeit – von der Kunst, der Diener mehrerer Herren zu sein

Kooperative Betriebsmodelle zur gemeinsamen Nutzung von IT-Systemen und Programmen gewinnen in Wirtschaft und Verwaltung immer größere Bedeutung. Sei es im Zuge von E-Government-Projekten, beim Betrieb von Rechenzentren, der Modellierung von Datenbanksystemen oder dem „Griff in die Cloud" (siehe hierzu auch Seite 87), häufig stellt der gemeinschaftliche Betrieb oder die Nutzung eines zentralen Dienstleisters bei der Realisierung von IT-Vorhaben eine ernsthafte Alternative zum mehrfachen lokalen Vorhalten entsprechender Infrastrukturen dar.

Die Chance zum optimierten Ressourceneinsatz birgt jedoch auch neue, systemimmanente Risiken. Insbesondere bei der Verarbeitung personenbezogener Daten bedarf es in diesem Umfeld besonderer Überlegungen, um den Anforderungen der informationellen Gewaltenteilung zu genügen, den Grundsatz der Zweckbindung aufrecht zu erhalten und das gebotene Maß an Vertraulichkeit herzustellen. Sobald im datenschutzrechtlichen Sinne verschiedene verantwortliche Stellen, die sogenannten Mandanten, beteiligt sind und ein solcher Zwang zur logischen Trennung bei Verarbeitung, Konfiguration und Zugriffsberechtigung entsteht, wird die Mandantenfähigkeit entsprechender Verfahren vorausgesetzt.

Eine Hilfestellung

Dass es an eindeutigen Definitionen und begleitenden Erläuterungen hierzu sowie dem Verständnis für die Grundproblematik fehlte, war im Laufe verschiedener auch länderübergreifender Beratungsgespräche und Prüfungen – insbesondere im Bereich von Krankenhäusern, bei IT-Dienstleistern und bei konsolidierten Rechenzentren für gleichartige Kundenbereiche im öffentlichen Bereich – immer wieder festzustellen. Um hier zu einer einheitlichen Definition und einer einheitlichen Prüfpraxis zu gelangen, verabschiedete die Datenschutzkonferenz des Bundes und der Länder im November 2012 die vom Arbeitskreis Technik vorgelegte Orientierungshilfe „Mandantenfähigkeit". Hiermit soll sowohl den verantwortlichen Stellen, als auch den Entwicklern und Anbietern entsprechender Verfahren und Systeme der Weg zu datenschutzgerechten Lösungen aufgezeigt werden.

Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit –: www.lfd.niedersachsen.de/ >Technik und Organisation >Orientierungshilfen und Handlungsempfehlungen >Mandantenfähigkeit

Zur Definition

Der Begriff „Mandant" oder „Mandantenfähigkeit" wird häufig verwendet, wenn es Unternehmen, Behörden oder Organisationen ermöglicht werden soll, Daten in einer Datenbank logisch zu trennen und zu verwalten. Mit Hilfe der Mandantenfähigkeit können z. B. Daten verschiedener Abteilungen einer Organisation/eines Unternehmens oder verschiedener Kunden eines IT-Services/Rechenzentrums getrennt vorgehalten werden. Die Datenschutzgesetze der Länder und des Bundes fordern jedoch, dass personenbezogene Daten,

die zu unterschiedlichen Zwecken erhoben worden sind, getrennt voneinander verarbeitet werden. Die getrennte Verarbeitung betrifft sowohl die Speicherung als auch die Verarbeitungsfunktionen wie etwa Datenbanktransaktionen oder Datensatzbuchungen.
Aus wirtschaftlichen oder praktikablen Gründen kann es aber sinnvoll sein, dass Ressourcen wie Hard- und Software, also IT-Infrastrukturen für verschiedene, voneinander zu trennende Datenbestände gemeinsam genutzt werden. In begründeten Fällen kann daher auch eine gemeinsame Speicherung mit mandantenbezogener Kennzeichnung der Daten zulässig sein. Voraussetzung hierfür ist, dass die Daten mandantenbezogen geführt und Verarbeitungsfunktionen, Zugriffsberechtigungen und Konfigurationseinstellungen je Mandant eigenständig festgelegt werden können. Die Datenverarbeitung muss dabei zwingend durch technische Maßnahmen getrennt voneinander erfolgen. Insbesondere gilt das auch dann, wenn für die jeweiligen Daten unterschiedliche Stellen verantwortlich sind oder es sich bei den personenbezogenen Daten um besondere Arten personenbezogener Daten handelt.

Konkrete Fälle betreffen Polizei, Krankenhäuser und Schulen

Die ersten konkreten Fälle, in denen sich Verfahrensverantwortliche und deren Dienstleister und Softwareanbieter mit IT-Verfahren der Frage ausgesetzt sahen, wie ein datenschutzrechtlich beanstandungsfreies Design dieser Verfahren aussehen würde, hatte ich bereits 2012 zu begutachten. Ein Fall betraf und betrifft das Verfahren zur Erfassung und Auswertung der Telekommunikationsüberwachung der Polizei des Landes Niedersachsen (siehe gesonderter Beitrag auf Seite 106), bei dem die Software eines Softwareanbieters anzupassen ist. In weiteren Fällen betraf diese Thematik auch bundesweit die IT-Systeme der Kliniken, so genannte Krankenhausinformationssysteme (KIS), bei denen dem Trennungsgebot und der Zweckbindung entsprechende technische Anforderungen zu prüfen sind, sei es in den logischen Schichten der Anwendungssoftware, des Datenbankmodells mit verschiedenen Tabellen, Views und Zugriffsberechtigungen verschiedener Rollen, der Betriebssystemebene, der Virtualisierung oder ebenso der Infrastruktur und der Hardware.
Auch im Bereich der inzwischen zahlreich anzutreffenden oder in Planung befindlichen Schulserversystemen ergeben sich in den meisten Fällen eine große Zahl von Fragen zur Mandantentrennung auf verschiedenen Ebenen – etwa der Trennung zwischen mehreren Schulen, zwischen Schuljahrgängen, zwischen Schulklassen, zwischen Arbeitsgruppen und temporären Formationen.
Die bei den häufigen Beratungen und bei Prüfungen anzutreffenden Kenntnisse über die strukturellen Anforderungen einer datenschutzkonformen Mandantenfähigkeit solcher Verfahren sind häufig sehr eingeschränkt. Das trifft vor allem auf verantwortliche Personen zu, die mit dem Datenschutzrecht und den technischen Details weniger vertraut sind. Leider ist jedoch selbst bei erfahreneren Personen – sei es unter den behördlichen Datenschutzbeauftragten, den für die IT-Einführung und den Betrieb beauftragten Technikern, bei den IT-Sicherheitsbeauftragten und sogar bei den Anbietern von Software oder Anbietern vollständiger Lösungen – nicht immer bekannt, dass im Zusammenhang mit komplexen Lösungen die Informationen, die verschiedenen Kunden/Mandanten zuzuschreiben sind, dem Gebot der strikten Trennbarkeit und jederzeitigen Herauslösbarkeit einzelner Mandanten unterworfen sein müssen. Bei den Lösungsanbietern, die bereits eine am

Markt verfügbare, häufig sogar auf die Prozesse bezogen vorkonfektionierte Fachanwendung anbieten, stellt sich bisweilen heraus, dass im Kern des Produktdesigns, insbesondere des Datenbankdesigns, diese Trennungserfordernisse nicht von vornherein eingeplant waren. Eine nachträgliche Änderung dieser Prinzipien würde mithin einen aufwändigen und kostenintensiven Eingriff erfordern. Dies zeigt einmal mehr, wie sehr mein für die IT-Entwicklung favorisierter Ansatz des „privacy-by-design" an der Erfolgsfrage beteiligt ist, ob Software-, Anwendungs- und Lösungsentwickler von vornherein datenschutzkonforme und datenschutzfreundliche Technologien, Lösungsbaukästen und damit Anwendungen entwickeln können, die auch einer Datenschutzrevision standhalten.

Im Produktdesign müssen Trennungserfordernisse für Informationen, die verschiedenen Kunden/Mandanten zuzuschreiben sind, eingeplant sein.

In fünf Prüfschritten zu einem Plan

Mit der genannten Orientierungshilfe der DSB-Konferenz empfehlen wir eine systematische Vorgehensweise mit fünf Prüfschritten, um den Handlungsbedarf festzustellen:

- Prüfschritt 1: Rechtliche Grundlagen
- Prüfschritt 2: Ausgestaltung von Übermittlungen zwischen Mandanten
- Prüfschritt 3: Abgeschlossenheit der Transaktionen innerhalb eines Mandanten
- Prüfschritt 4: Unabhängigkeit der Konfiguration
- Prüfschritt 5: Beschränkung der mandantenübergreifenden Verwaltung der Datenverarbeitung

Die Details dieser Vorgehensweise werden in der Orientierungshilfe näher erläutert.

Auf Basis dieser Vorüberlegungen ist dann das Datenschutz- und Sicherheitsmanagement auf diese besondere Form der Datenverarbeitung anzupassen. In der Konzeption und der Umsetzung des Datenschutzmanagements empfehlen wir dabei die Durchführung einer Risikoanalyse, den Nachweis ausreichender angemessener Sicherheits- und Datenschutzmaßnahmen (gem. § 7 NDSG bzw. § 9 BDSG und Anlage) sowie eine vollständige Dokumentation und eine anschließende Restrisikobetrachtung. So lässt sich das Ziel der Nachvollziehbarkeit und Gewährleistung der Vollständigkeit gewährleisten.

Zentralisierung der Telekommunikationsüberwachung

Das Telekommunikationsgesetz (TKG) und die Strafprozessordnung sehen 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 im Niedersächsischen Gefahrenabwehrgesetz ebenfalls Rechtnormen, die die TKÜ erlaubt. Da die Daten zu einem erheblichen Anteil personenbezogene Daten beinhalten, die unter die höchste Schutzstufe E nach dem von mir veröffentlichten Schutzstufenkonzept fallen und die TKÜ einen erheblichen Eingriff in die Grundrechte der Bürger mit sich bringt, sind die Erlaubnistatbestände im Gesetz mit entsprechend ausgestalteten Hürden und strengen Verfahrensregeln – etwa dem Richtervorbehalt – geregelt.

§ 100a Strafprozessordnung (StPO) (Telekommunikationsüberwachung und -aufzeichnung) sowie §§ 100b bis 100d, 110f und 100g, 100i, 161, 163, 483 bis 485, 487 und 489 StPO

§ 33a Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG) (Datenerhebung durch Überwachung der Telekommunikation)

Telekommunikationsgesetz (TKG):
§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden
§ 112 Automatisiertes Auskunftsverfahren
§ 113 Manuelles Auskunftsverfahren

Seitdem neben der klassischen Telefonie der technischen Entwicklung folgend zahlreiche Kommunikationsvorgänge über das Internet geleitet werden und zudem verschiedene Internet-Plattformen und -Dienste genutzt werden, wächst auch das Maß der Nutzung digitaler Medien für kriminelle Zwecke, sei es zur Vorbereitung einer Straftat oder auch um das Internet als Tatmittel oder Tatgegenstand zu nutzen. Die Polizeiliche Kriminalstatistik des Bundeskriminalamts (BKA) und des Landeskriminalamtes Niedersachsen (LKA NI) weisen seit Jahren zudem entsprechende Zuwachsraten und immer neue Phänomene bei Delikten der Computerkriminalität im weiteren Sinne auf. Dementsprechend entwickelte sich parallel auch die Notwendigkeit für die Ermittlungsbehörden, im Fall der TKÜ nicht nur die analoge Kommunikation, sondern auch den digitalen Kommunikations- und Datenverkehr, der über Internettechnologie erfolgt (IP-Verkehr), mit allen bekannten technischen Diensten zu überwachen, sofern dies nach den gesetzlichen Vorschriften zur Strafverfolgung oder Gefahrenabwehr zulässig ist.
Das LKA NI ist seit April 2009 vom Niedersächsischen Ministerium für Inneres und Sport mit einer Planung für eine neue TKÜ-Anlage zur Nutzung durch das LKA NI und alle sechs Flächen-Polizeidirektionen des Landes Niedersachsen beauftragt worden. Die neue Anlage soll im Rahmen eines erneuerten „Verwaltungsabkommens über die Kooperation beim Betrieb der Internetüberwachungstechnik zwischen den Ländern Niedersachsen und Bremen“ zudem der Mitnutzung durch die Polizei des Landes Bremen dienen. Dabei wird in der gesetzlich vorgeschriebenen Vorabkontrolle (§ 7 Abs. 3 NDSG) von einer Datenübermittlung gemäß § 487 StPO im Fall einer Strafverfolgung und gemäß § 41 Nds. SOG im Fall einer Gefahrenabwehrmaßnahme ausgegangen. Auftragsgemäß hat das LKA 2009 ein Grobkonzept und eine Leistungsbeschreibung für die fachliche und die technische Seite erstellt. Die Vorabkontrolle wurde im September 2010 durchgeführt.

Küstenländer planen TKÜ-Rechen- und Dienstleistungszentrum Nord – Kooperation läuft bereits

Parallel zu dem Erneuerungsvorhaben in Niedersachsen planen die Innenminister und -senatoren der Bundesländer Bremen, Hamburg, Niedersachsen, Schleswig-Holstein und Mecklenburg-Vorpommern seit 2008 die Prüfung von länderübergreifenden Kooperationen und

für Niedersachsen – und für Bremen

schließlich 2010 die Einrichtung eines gemeinsamen „TKÜ-Rechen- und Dienstleistungszentrums im Verbund der norddeutschen Küstenländer“ (TKÜ-RDZ Nord). Die Gründe werden einvernehmlich ebenfalls in der rasanten technischen Entwicklung und der zunehmenden Verlagerung der Telekommunikation in das Internet gesehen, weshalb die Instrumente für die Erkenntnisgewinnung der Sicherheitsbehörden den veränderten Gegebenheiten anzupassen seien. Zudem werden ökonomische Gründe für eine Erzielung von Synergieeffekten bei einer Ressourcenteilung gesehen sowie die Chance zur Optimierung der Verfügbarkeit der Systeme und Verfahren. Von dem Vorhaben erfuhr ich durch die LfDI Bremen etwa einen Monat vor der schriftlichen Information seitens des LKA NI am 21.10.2011, mit der ich zu einem Informationsgespräch durch den Projektleiter am 18.11.2011 eingeladen wurde. Dort wurden der Projektauftrag und der damalige Arbeitsstand erläutert.

Das Projekt TKÜ-RDZ Nord ist in zwei Phasen aufgeteilt:

Phase 1: Aufbau einer technischen Kooperation der Länder zur Schaffung von erforderlichen Kompensationsmöglichkeiten beim Ausfall der ländereigenen TKÜ-Anlagen und eines sofortigen Ausgleichs bei Lastspitzen eines Landes im Bereich der IP-basierten TKÜ

Phase 2: Erstellung eines Umsetzungskonzeptes zur vollständigen Zentralisierung der TKÜ in einem Rechen- und Dienstleistungszentrum (RDZ) TKÜ Polizei an den Standorten Hannover und Hamburg zu einem redundant ausgelegten TKÜ-System.

In einer ersten Stellungnahme machte ich bei dem Präsentationstermin deutlich, dass ich es aus datenschutzrechtlicher Sicht für unabdingbar halte, in der Verfahrensausgestaltung den sogenannten Kernbereichsschutz gem. § 100a Abs. 4 Strafprozessordnung (StPO) ausschließlich durch die jeweils verantwortliche Stelle prüfen und bestimmen zu lassen.

Landesdatenschutzbeauftragte richten Kooperations-AG ein

Angesichts der weitreichenden und länderübergreifenden Wirkung des Vorhabens war auch nach meiner Auffassung eine Kooperation der Datenschutzaufsichtsbehörden anzustreben. Die technischen Bereiche der Landesdatenschutzbeauftragten der beteiligten Länder richteten eine Kooperations-AG ein, in der bereits am 24.11.2011 erstmals das Ziel arbeitsteiligen Vorgehens und einer abgestimmten Positionierung im Interesse einer möglichst einheitlichen und zeitnahen Stellungnahme gegenüber den Verfahrensverantwortlichen des Projektes TKÜ-RDZ Nord vereinbart wurde. Am 27.1.2012 wurde das Thema in einem weiteren Arbeitsgespräch fortgesetzt.

Erst die Rechtsgrundlagen und das Fachverfahren, dann die Technik!

Die Rechtsgrundlage kann bei länderübergreifender Aufgabenübertragung grundsätzlich nur ein Gesetz sein, das in Form eines Staatsvertrags mit Ratifizierung in den Ländern erlassen wird.

Eine wichtige Kernfrage wurde im Februar 2012 schriftlich an die Projektgruppe gerichtet: Aus Sicht der Landesdatenschutzbeauftragten der beteiligten Länder ist bei der Ausgestaltung des Vorhabens von zentraler Bedeutung, ob es sich bei den Leistungen, die das gemeinsame Zentrum für die beteiligten Länder erbringt, um eine Datenverarbeitung im Auftrag im Sinne der Landesdatenschutzgesetze oder um eine so genannte Funktionsübertragung handelt. Diese Abgrenzung hat Folgen für die Rechtsgrundlage der Datenverarbeitung im Rahmen der Kooperation. Während die Weitergabe von personenbezogenen Daten im Rahmen einer Datenverarbeitung im Auftrag auf Grundlage eines Vertrages zulässig ist, handelt es sich bei einer Funktionsübertragung beim Empfänger der Daten um eine eigenständige verantwortliche Stelle. Die Weitergabe der Daten an den Empfänger stellt datenschutzrechtlich eine Übermittlung dar, für die es einer Übermittlungsbefugnis bedarf. Grundvoraussetzung ist, dass der empfangenden Stelle die Aufgaben rechtmäßig übertragen wurden. Für die Übertragung von Aufgaben von einer Stelle an eine andere Stelle bedarf es einer besonderen Rechtsgrundlage. Dies kann bei länderübergreifender Aufgabenübertragung grundsätzlich nur ein Gesetz sein, das in Form eines Staatsvertrags mit Ratifizierung in den Ländern erlassen wird. Dies ist letztlich eine staatsorganisationsrechtliche Frage, die aber Auswirkungen auf die Rechtmäßigkeit der Datenverarbeitung durch das TKÜ-Zentrum hat.
Im April 2012 legte das Projekt einen Vertrag zur Auftragsdatenverarbeitung („Datenverarbeitungsauftrag für die technische Kooperation bei der Telekommunikationsüberwachung der Polizeien im Verbund der norddeutschen Küstenländer“) vor. Am 25.4.2012 erläuterte ich in einem Mängelbericht an den Präsidenten des LKA NI das Zwischenergebnis unserer Überprüfungen und Verbesserungsvorschläge. Gleichlautende Schreiben wurden von den Landesdatenschutzbeauftragten (DSB) in den anderen vier Bundesländern an die dortige Polizeiführung gesandt. Die Bekanntgabe eilte, weil die Phase 1 der Kooperation mit der Unterzeichnung des entsprechenden Vertrages am Folgetag starten sollte.

Mängelbericht des DSB mit Verbesserungsvorschlägen

Der Stand der bis dahin durch die DSB erfolgten gemeinsamen Prüfung und Bewertung der fachlichen und technischen Konzeptionen sowie des tatsächlichen Iststandes bei der Erarbeitung der betrieblichen Details ließ nach gemeinsamer Überzeugung der DSB der fünf betroffenen Länder erkennen, dass der Projektstatus nicht den erforderlichen Reifegrad bezüglich der Informationssicherheit und der datenschutzrechtlichen Schutzmaßnahmen im technisch-organisatorischen Bereich erreicht hat, der für einen vertretbaren Betrieb mit Echtdaten unverzichtbar ist. Im Ergebnis empfahlen die DSB, für den weiteren Fortgang des Projektes solange auf die Erteilung von Einzelaufträgen an das LKA Hamburg und damit auf die dortige Datenverarbeitung im Auftrag zu verzichten, bis die im Detail genannten Mängel behoben und die datenschutzrechtlichen Bedenken ausgeräumt sind. Die kritischen Faktoren bezogen sich zu diesem Zeitpunkt auf folgende Hauptaspekte (auf Details wird an dieser Stelle verzichtet):

- Der Schutzbedarf der personenbezogenen Daten beschränkte sich unzulässigerweise auf eine pauschale Festlegung der Schutzstufe „normal“, analog zum Fahndungssystem der Polizeien, ohne eine sachgerechte, vollständige, den Umfang und die Umstände der Da-

tenverarbeitung berücksichtigende Schutzbedarfsfeststellung. Insbesondere die Tatsache, dass bei TKÜ-Fällen die Überwachungsmaßnahmen nach dem Strafprozessrecht und dem Gefahrenabwehrrecht weitgehende Grundrechtseingriffe mit sich bringen und Inhaltsdaten von Sprachkommunikation aufgezeichnet werden, die auch den Kernbereich privater Lebensumstände beinhalten können, lässt deutlich werden, dass die Schutzstufe mindestens mit „hoch" einzustufen ist. Eine Objektivierung des Schutzbedarfes ist Grundvoraussetzung, und Fehleinschätzungen bereits an der Basis würden in der Folge zu potenzierenden Fehleinschätzungen bei der Risikobewertung und bei der Planung der Schutzmaßnahmen nach sich ziehen.

- Zweifel an der Vollständigkeit und inhaltlichen Belastbarkeit des IT-Sicherheitskonzepts bezogen auf die tatsächliche Tragweite und Risikolage des IT-Verfahrens.
- Der Basis-Sicherheitscheck sollte erst im Herbst 2012 abgeschlossen sein und käme damit zu spät.
- Es bestanden Zweifel an der Vollständigkeit der Strukturanalyse gem. BSI-Standard 100-2.
- Die Modellierung zum IT-Sicherheitskonzept war unvollständig.
- Unzulässige Inbetriebnahme vor Abschluss der Arbeiten: Der Katalog der technisch-organisatorischen Maßnahmen zur Erreichung der datenschutzrechtlichen Schutz-, Sicherheits- und Gestaltungsziele gemäß den Landesdatenschutzgesetzen (LDSG; z. B. § 7 Abs. 1 NDSG) ist mit sehr hoher Wahrscheinlichkeit unvollständig.
- Zur Gewährleistung der Mandantenfähigkeit der Anwendung durch eine korrekte Implementierung wurde den Projektvertretern die kurz vor Freigabe befindliche Entwurfsversion der „Orientierungshilfe Mandantenfähigkeit"

des AK Technik der DSB-Konferenz vom 5.4.2012 überreicht. Diese waren in der Architektur und im fachlichen und im technischen Feinkonzept sowie in die IT-Sicherheitskonzeption noch einzuarbeiten (vgl. Seite 103).
- Insgesamt war die Dokumentenlage noch unvollständig, eine Revisionsfähigkeit war folglich nach diesem Stand weder planmäßig noch betrieblich mit Echtdaten möglich.

Zur Nachbesserung der genannten Mängel wurde der Projektgruppe empfohlen, sieben näher erläuterte Prozessschritte für die Vervollständigung technisch-organisatorischen Datenschutzmaßnahmen zu vollziehen. Die Länder haben mit Hamburg und mit Niedersachsen inzwischen Auftragsdatenverarbeitungsverträge geschlossen, in denen die Rahmenbedingungen für eine tatsächliche Übernahme einer Telekommunikationsüberwachung geregelt werden. Für die zweite Phase des Projektes steht noch die Erstellung eines Konzeptes für die vollständige Zentralisierung der TKÜ ab dem Jahr 2016 aus. Dann soll es den Plänen zufolge ein gemeinsames Zentrum für die fünf beteiligten Länder Hamburg, Niedersachsen, Mecklenburg-Vorpommern, Bremen und Schleswig-Holstein geben, in dem alle TKÜ-Maßnahmen zentralisiert durchgeführt werden. Nach übereinstimmender Ansicht der Landesdatenschutzbeauftragten dieser Länder sollte die rechtliche Konstruktion dieses gemeinsamen Zentrums, die Verantwortlichkeit für die Datenverarbeitung und die Verteilung der Aufgaben durch einen Staatsvertrag geregelt werden, um mit der Ratifizierung durch die Landesgesetzgeber eine gesetzliche Grundlage für die Zentralisierung zu schaffen.

Auch zahlreiche Mängel beim TKÜ-Verfahren im LKA NI

Im weiteren Verlauf stellten sich zum Datenschutzkonzept für das TKÜ-Verfahren des LKA NI, auch vor dem Hintergrund der Verwaltungsvereinbarung mit der Freien Hansestadt Bremen, ähnliche Fragen wie zu dem geplanten TKÜ-RDZ Nord. Der Unterschied lag darin, dass es sich bei dem TKÜ-Verfahren bereits um den konkreten Aufbau eines neuen Systems handelte. Insofern ließen sich einerseits vorbildhafte Strukturen und die Umsetzung von Anforderungen erproben und andererseits ggf. aus Fehlern lernen. Bereits hier geht es insbesondere um die rechtlichen Fragen zum Erfordernis eines Staatsvertrages und zur datenschutzrechtlich beanstandungsfreien Mandantenfähigkeit unter Beachtung des Trennungsgebotes zwischen den Ländern und den jeweiligen personenbezogenen Daten.
Auf der Grundlage von Informationen der LfDI Bremen wurde das LKA NI am 5.10.2012 gebeten, die fehlenden Dokumente zur Konzeption vorzulegen. Insbesondere halte ich in solchen Verfahren für erforderlich:
- Schutzbedarfsfeststellung,
- Risikoanalyse,
- aus Sicht des Landes Bremen Vertrag zur Datenverarbeitung im Auftrag nach § 9 Bremisches Datenschutzgesetz,
- Beschreibung der getroffenen technischen und organisatorischen Maßnahmen,
- IT-Sicherheitskonzept,
- Betriebskonzept,
- Verfahrensbeschreibung aller Systeme zur Aufzeichnung und Verarbeitung der Überwachungsmaßnahmen,
- dazugehörige Berechtigungskonzepte und Administrationskonzepte,

- Fachkonzeption,
- Beschreibung der Verschriftung der Gesprächsinhalte,
- Beschreibung der sicheren Übertragung der Daten und der dafür eingesetzten zertifizierten Komponenten.

Am 11.10.2012 nahmen meine Mitarbeiter sowie Vertreterinnen der LfDI Bremen das IT-Verfahren der TKÜ-Zentrale beim LKA Niedersachsen in Augenschein. In dem vorläufigen Prüfbericht vom 3.12.2012 wurden die 14 vorhandenen Dokumente zum Projekt mit dem bis dahin bekannten Bearbeitungsstand für die Bewertung zugrunde gelegt. Im Wesentlichen ergaben sich schließlich Mängel in folgenden sieben Themenblöcken:

1. Die Aussagen zur Risikoanalyse, auch nach Berücksichtigung des Überarbeitungsstandes vom 18.10.2012, sind noch unvollständig. In der Folge war nicht bestimmbar, ob alle erforderlichen Maßnahmen gemäß § 7 Abs. 2 NDSG getroffen worden sind.
2. Die erforderliche Mandantenfähigkeit des Verfahrens im datenschutzrechtlichen Sinne ist nicht erwiesen. Die Beschreibung hierzu lässt erkennen, dass es einer strukturellen Nachbesserung bedarf.
3. Das Rechte-Rollen-Konzept ist zu vervollständigen.
4. Die Protokollierung ist um die fehlenden Komponenten und Maßnahmen zu ergänzen.
5. Die Dokumentenlage ist in Teilen lückenhaft, so dass weder der gesicherte und rechtssichere Betrieb, noch eine Revisionssicherheit gewährleistet werden können.
6. Aufgrund des festgestellten sehr hohen Schutzbedarfes sind Inhalts- und Verkehrsdaten zu verschlüsseln.
7. Die Fernwartung ist nur mit besonderen, der Schutzstufe „sehr hoch“ angemessenen Sicherheitsmaßnahmen, zulässig.

Die Details der Mängel wurden in einem 52-Punkte-Anforderungskatalog beschrieben. Im Ergebnis wies ich darauf hin, dass ein Echtbetrieb mit der Verarbeitung personenbezogener Daten daher bis zur Fertigstellung der dort genannten Maßnahmen unterbleiben müsse. Auch hier erhielt das LKA Bremen im Zuge der kooperativen Zusammenarbeit ein inhalts- und zeitgleiches Schreiben der LfDI Bremen. Mit seinem Antwortschreiben signalisierte der Präsident des LKA NI am 19.12.2012 weiteren Gesprächsbedarf. Eine Besprechung wurde schließlich für den 12.2.2013 vereinbart. Über den Fortgang zu diesem Verfahren im folgenden Berichtszeitraum werde ich im nächsten Tätigkeitsbericht Stellung nehmen.

Gemeinsame norddeutsche Beratung und Prüfung: IT-Dienstleister Dataport

Dataport ist eine rechtsfähige Anstalt des öffentlichen Rechts (AöR) mit Hauptsitz in Altenholz und fünf weiteren Niederlassungen und wurde zum Jahresbeginn 2004 gegründet. Trägerländer sind die Bundesländer Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen und Schleswig-Holstein. Ziel ist es, in einem internen Verhältnis Aufträge für IT-Dienstleistungen ohne aufwändige Vergabeverfahren erteilen zu können, was zu Synergieeffekten mit Kostensenkungen und Effizienzsteigerungen führen soll. Damit folgen die Trägerländer ebenfalls dem Prinzip, kooperative Betriebsmodelle zur gemeinsamen Nutzung von IT-Systemen und Anwendungsprogrammen zu schaffen. Diese gewinnen nicht nur in der Wirtschaft, sondern auch in der öffentlichen Verwaltung eine immer größere Bedeutung. Im öffentlichen Dienst geschieht dies seit einigen Jahren zum einen durch übergreifende E-Government-Projekte, aber auch im IT-Betrieb von Rechenzentren, bei der Modellierung von Datenbanksystemen oder beim Betrieb gemeinsamer oder verteilter Cloud-Architekturen (vgl. Beitrag Cloud Seite 87).

Dataport nimmt die Aufgabe eines Informations- und Kommunikationsdienstleisters wahr für Sprach- und Datenkommunikation, Entwicklung und Betrieb von Verwaltungsfachanwendungen, die Erstellung von Datenschutz- und Sicherheitskonzepten sowie IT-Fortbildung der öffentlichen Verwaltung[1] für alle Länder außer Mecklenburg-Vorpommern und Niedersachsen. Für letztere ist Dataport ausschließlich Dienstleister für die Steuerverwaltungen. Das Land Niedersachsen wird damit den Betrieb seiner steuerlichen Verfahren zum sogenannten „Konsens-1-Verfahren“ durch die bei Dataport im Data Center Steuer (DCS) dafür vorhandene technische Infrastruktur durchführen lassen. Für diese länderübergreifende Dienstleistung bedurfte es gesetzlicher Grundlagen, weil nach dem föderalen Prinzip jedes Land eigene Zuständigkeiten wahrnimmt, eine länderübergreifende Aufgabenwahrnehmung also eine Abweichung von diesem Prinzip darstellt, was ohne gesetzgeberische Erlaubnis nicht rechtskonform wäre. Daher wurde 2003 zum Beginn des Jahres 2004 ein Staatsvertrag[2] abgeschlossen, der aufgrund des Parlamentsvorbehaltes der beteiligten Gesetzgeber durch ein Gesetz zu verabschieden war:

- Die Länder Mecklenburg-Vorpommern und Bremen wurden auf diesem Weg mittels Staatsvertrag 2006 drittes und viertes Beitrittsland.
- Das Land Niedersachsen wurde zum 1.1.2010 fünftes Trägerland.[3] Das Land Sachsen-Anhalt trat als sechstes Land zum Jahreswechsel 2013 bei.[4]

1 Dataport nennt sich „Full Service Provider für Informationstechnik der Verwaltung“ (http://www.dataport.de/ueber-uns/unternehmen/Seiten/default.aspx)

2 Staatsvertrag zwischen dem Land Schleswig-Holstein und der Freien Hansestadt Hamburg über die Errichtung von Dataport als rechtsfähige Anstalt des öffentlichen Rechts vom 27. August 2003 in der Fassung des Änderungsstaatsvertrags für den Beitritt des Landes Niedersachsen, unterzeichnet am 30. Oktober 2009 und 30. April 2010

3 Plenarprotokoll des Nds. Landtages Nr. 16/86 vom 9.11.2010 S. 10866 mit der einzigen (abschließenden) Beratung zum Entwurf eines Gesetzes zu dem Staatsvertrag zwischen dem Land Schleswig-Holstein, der Freien und Hansestadt Hamburg, dem Land Mecklenburg-Vorpommern, der Freien Hansestadt Bremen und dem Land Niedersachsen über den Beitritt des Landes Niedersachsen zur rechtsfähigen Anstalt des öffentlichen Rechts „Dataport“– Gesetzentwurf der Landesregierung

4 Redaktionelle Anmerkung: Der Beitritt Sachsen-Anhalts zum Dataport-Verbund erfolgte schließlich erst am 24.2.2014, weil die Ratifizierung durch die Parlamente erst im Februar 2014 abgeschlossen war. Der Staatsvertrag ist jedoch rückwirkend zum 1.1.2013 in Kraft getreten.

- Durch eine Übertragung von 50 Prozent des schleswig-holsteinischen Anteils am Stammkapital Dataports auf den IT-Verbund Schleswig-Holstein AöR (ITVSH) kam dieser mit Wirkung vom 1.1.2012 als weiterer Träger von Dataport AöR hinzu.

Chancen und Risiken

Aus datenschutzrechtlicher Sicht ist es einerseits begrüßenswert, wenn durch eine Konsolidierung die sektorspezifischen Aktionsbereiche des IT-Dienstleisters gestärkt werden, vorausgesetzt, dass dadurch die Professionalisierung insbesondere der IT-Sicherheit und der technisch-organisatorischen Datenschutzmaßnahmen profitiert und sich auch tatsächlich verbessert. Allerdings erfolgt Konsolidierung nicht nur nach Quantität, indem die großen Verfahren die Verfahrensweisen und technischen Abläufe bestimmen. Vielmehr müssen aus bereits gereiften kleineren Einzellösungen die sogenannten best practices nutzbar gemacht werden, also die Erfahrungen zur Optimierung von Prozessen und Technologien, die den Datenschutz und die IT-Sicherheit fördern. Zudem kommen durch die Zusammenlegung von Funktionen oder die Nutzung gemeinsamer Verfahren zusätzliche Risiken ins Spiel, die vollständig analysiert und für die alle angemessenen Schutzmaßnahmen getroffen werden müssen. Die erforderliche Abgrenzung zwischen den Ländern im Rahmen der Mandantenfähigkeit ist eine der entscheidenden Herausforderungen für Zusammenlegungen dieser Größenordnungen. (vgl. Beitrag Mandantenfähigkeit Seite 103).

Niedersachsen hat am 30. April 2010 den **Staatsvertrag zum Beitritt zu Dataport** unterzeichnet (Nds. GVBl Nr. 26/2010 S. 500)

Gesetz zum Staatsvertrag vom 10.11.2010 Gesetz- und Verordnungsblatt Nr. 26 18.11.2010 S. 500–506, Bekanntmachung über den Zeitpunkt des Inkrafttretens des Staatsvertrages vom 3.12.2010 Gesetz- und Verordnungsblatt Nr. 29, 7.12.2010, S. 549, In Kraft getreten am 26.11.2010

Welches Recht gilt?

Für die Errichtung und den Betrieb der Anstalt gilt das schleswig-holsteinische Landesrecht, soweit der Staatsvertrag nichts anderes bestimmt. Nach § 15 des Staatsvertrages gelten grundsätzlich für die Verarbeitung personenbezogener Daten durch Dataport und ihre Niederlassungen die Vorschriften des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG).
Für die Trägerländer gibt es jedoch Abweichungen. In § 15 Absatz 2c ist zum Beispiel geregelt: „Verarbeitet Dataport oder eine ihrer Niederlassungen personenbezogene Daten für öffentliche Stellen des Landes Niedersachsen, gelten dafür das Landesdatenschutzgesetz Niedersachsen (NDSG) und die sonstigen für öffentliche Stellen in Niedersachsen geltenden Vorschriften über den Datenschutz. Die oder der Landesbeauftragte für den Datenschutz Niedersachsen überwacht die Einhaltung dieser Vorschriften, berät Dataport und ihre Niederlassungen insoweit in Fragen des Datenschutzes und nimmt insoweit das Anhörungsrecht gegenüber der oder dem Datenschutzbeauftragten der Anstalt wahr. Beanstandungen nach § 23 NDSG richtet die oder der Landesbeauftragte für den Datenschutz Niedersachsen an das Finanzministerium Niedersachsen.“

Nach Abs. 5 lässt Dataport auch eine Kontrolle zu, wenn die Landesdatenschutzbeauftragten (LfD) der Trägerländer sich einvernehmlich wechselseitig mit der Durchführung der Überwachung beauftragen.

Kooperativem Betrieb folgt kooperative Aufsicht

Wenn föderale Länder per Staatsvertrag bei IT-Aufgaben zusammenarbeiten, liegt es nahe, die datenschutzrechtliche Beratung und Aufsicht ebenfalls in einem möglichst abgestimmten Verfahren zwischen den LfD gegenüber den Trägerländern und Dataport durchzuführen. Bereits im Dezember 2009 hatten die LfD eine gemeinsames Auditverfahren beim Dataport „Data Center Steuern" (DCS) in Rostock durchgeführt, bei dem auch ein technischer Mitarbeiter meiner Behörde beteiligt war. Die Beratungs- und Aufsichtsmaßnahme wurde absprachegemäß federführend vom ULD Schleswig-Holstein geleitet. Die konsolidierte Aktion hat sich als vorteilhaft erwiesen.
Die Landesdatenschutzbeauftragten haben schließlich vereinbart, in einer Arbeitsgruppe regelmäßig ein Koordinierungstreffen durchzuführen. Ziel ist es, einen Erfahrungsaustausch zwischen den Aufsichtsbehörden zu fördern sowie inhaltliche Abstimmungsergebnisse zu erarbeiten. Die LfD behalten dabei jedoch ihre jeweils eigene unabhängige Aufsichtsfunktion, wie sie von den rechtlichen Bestimmungen gefordert werden. Von September 2011 bis Januar 2013 wurden schließlich sechs dieser Sitzungen in Hamburg durchgeführt und verschiedene Bewertungsfragen des materiellrechtlichen und technisch-organisatorischen Datenschutzes erörtert, welche die IT-Infrastruktur, IT-Grundsatz- und Querschnittsverfahren, IT-Fachverfahren und Organisationsfragen von Dataport betrafen. Insbesondere standen folgende Themenschwerpunkte im Berichtszeitraum auf der Tagesordnung:

- Elektronisches Personenstandswesen, hier insbesondere das gemeinsame Verfahren bei Dataport der Länder HH, HB und S-H.
- Data Center Steuern, insbesondere die Ergebnisse der Nachkontrollen und das weitere Vorgehen zum Audit, das im Dezember 2009 begonnen hatte.
- Vereinheitlichte Anforderungen an Sicherheitskonzepte/Risikoanalysen (Security Service Level Agreement) und Administrationskonzepte.
- Gemeinsame Austauschplattform der LfD für länderübergreifende Fachverfahren.
- Anforderungen an Mandantenfähigkeit bei gemeinsamen Verfahren bzw. Nutzung gleicher Funktionalitäten (siehe Beitrag Mandantenfähigkeit, Seite 103).
- Maßnahmen bei Verfahren mit hohem Schutzbedarf.
- Maßnahmen für den Grundschutz nach BSI und Grenzziehungen aus datenschutzrechtlicher Sicht.
- Einbindung der LfD zur Beratung bei der Planung des neuen Rechenzentrums „RZ²".[5] Nach der Umsetzung des ZaBI-Konzeptes (Zielarchitektur Basis Infrastruktur) zum Rechenzentrum 2010 am Standort Kiel folgte bei Dataport mit dem Projekt RZ² die Umsetzung für den Neubau zweier baugleicher Rechenzentren an den Standorten Hamburg-Alsterdorf und Norderstedt, um die IT-Systeme aus den von Dataport genutzten Systemräumen in Altenholz, Bremen, Hamburg (Alsterdorf, Bramfeld, Rothenburgsort)

5 Weitere Informationen zum Projekt RZ² siehe http://www.dataport.de/unsereloesungen/infrastruktur/rechenzentrum/Sew/Projekt-RZ%c2%b2.aspx

und dem Kieler ZaBI-RZ in modernen, ausbaufähigen Gebäuden zusammenzuführen. Ziele sollen unter anderem maximale Verfügbarkeit und Sicherheit sein. Der Betrieb ist inzwischen in Teilen aufgenommen worden.

- „KoPers Kommunal", ein integriertes Personalmanagementsystem (vorwiegend in Schleswig-Holstein im Einsatz, Einsatzerwägung in Bremen).
- Verfahren der Kommunen zum (neuen) elektronischen Personalausweis (nPA), Bewertungen von Konzepten zu den nPA-Berechtigungszertifikaten.
- Nutzung von Microsoft SharePoint.
- Standardisierung OSCI und xTA-WS als Webservice zur Anbindung an die XÖV-Transport-Infrastruktur.
- Managed Mobile Devices (zentral administrierte mobile Endgeräte wie Smartphones, Tablet-PC) mit Excitor DME; Problematik bei der Einbindung privater Smartphones; Risiken zu verschiedenen Betriebssystemplattformen.
- Microsoft Active Directory (AD); datenschutzrechtliche Fragen zu einer Konzeption, die eine einzige länderübergreifende Domain anstrebt.

Zeitweise wurden zu den gemeinsamen Arbeitssitzungen auch Vertreter der Dataport AöR für einen direkten fachlichen Austausch eingeladen.

Printzentrum Lüneburg – IT-Sicherheit durch Synergie

Das Land Niedersachsen hat seinen Anteil am Stammkapital durch Einbringung des Printzentrums Lüneburg (heute Dataport Druck- und Kuvertierzentrum) einschließlich Personal, Gebäude, Infrastruktur und IT-Hard- und Software geleistet (Landtags-Drucksache 16/3356). Gemäß Staatsvertrag war das Printzentrum Lüneburg bis 31.12.2012 zu überführen, als eine Niederlassung Dataports in Lüneburg zu führen und als Standort langfristig zu erhalten. Nach Aussage der Landesregierung sei die Schaffung eines zweiten Druckstandortes als Back-up-Lösung und zur Kapazitätserweiterung notwendig gewesen. Auch das bestehende Druckzentrum Dataports in Altenholz habe zunehmend an seiner Kapazitätsgrenze gearbeitet. Zudem habe es für den Fall technischer Störungen dort kein Back-up-Druckzentrum gegeben. Die Einbringung des bisher von Niedersachsen betriebenen Printzentrums bei Dataport eröffne daher die Möglichkeit einer insgesamt kostengünstigeren Bereitstellung von Druckleistungen und eine Erhöhung der Sicherheit in Ausfallsituationen für alle beteiligten Länder.[6] Aus Sicht der Informationssicherheit ist die Verfügbarkeit als Sicherheitsziel damit strukturell erhöht worden. Verfügbarkeit als Schutzziel des Datenschutzes partizipiert damit prinzipiell ebenfalls.

Fachlicher Austausch der Landesdatenschutzbeauftragten unabdingbar

Es wird einhellig davon ausgegangen, dass der fachliche Austausch der Landesdatenschutzbeauftragten bei einer kooperativen Aufsicht gegenüber Dataport unabdingbar ist, um zu möglichst zeitnah abgestimmten Beratungen und Kontrollen zu kommen, die eine verlässliche und gleichbleibend hohe Qualität aufweisen. Dataport ist an einheitlichen Bewertungen und Vorgaben interessiert. Bei gemeinsamen Verfahren bleibt es bisweilen sehr anspruchsvoll, dem Spannungsverhältnis zwischen landesspezifischen gesetzlichen Anforderungen und verfahrenstechnischen Vereinheitlichungen gerecht zu werden. Die Arbeitsgruppentreffen werden im Interesse dieser Abstimmungsprozesse daher weiterhin erfolgen.

6 Drucksache 16/3356 (siehe rechte Spalte)

4 Schwerpunktthema: Soziale Netzwerke

Soziale Netzwerke:
Kontrollverlust und Rechtsverstöße all inclusive

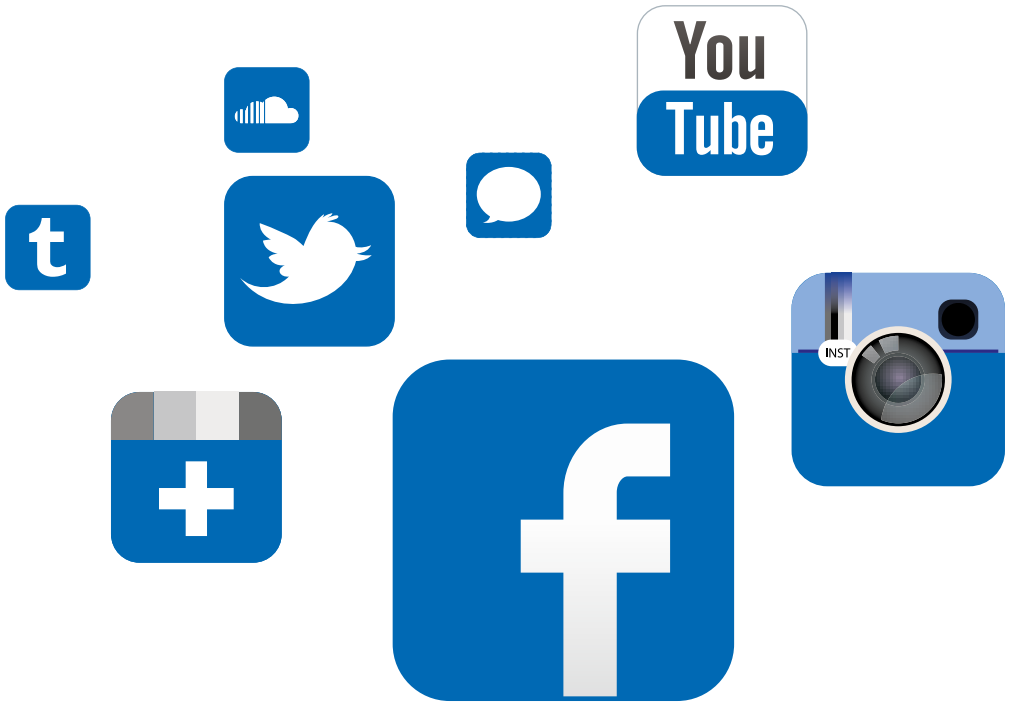
In meinen letzten beiden Tätigkeitsberichten ab 2007 habe ich bereits ausführlich über die Entwicklung der Plattformanbieter für soziale Medien und den Begleiterscheinungen für die informationelle Selbstbestimmung berichtet. Inzwischen hat sich der Markt erheblich zu Gunsten des US-amerikanischen Anbieters Facebook verlagert. Damit haben sich die meisten Nutzer – auch in Deutschland[1] rund 24 Millionen – dafür entschieden, ihre privatesten Angaben, Fotos, Lebensläufe, Kommunikationsverläufe und sozialen Kontaktinformationen dem US-Dienstanbieter Facebook anzuvertrauen. Dieses Unternehmen, das in seinen Rechenzentren mit Hochleistungskapazitäten und umfangreichen Funktionen angetreten ist, die Profile von inzwischen mehr als einer Milliarde Menschen auszuwerten, hat faktisch durch eine Vielzahl von Gadgets und der Verknüpfung von Daten das Prinzip der Privatheit und der Kontrolle personenbezogener Daten in Frage gestellt.

Facebook ist angetreten, die Welt glücklicher zu machen. Facebook ist andererseits aber auch ein Wirtschaftsunternehmen und verdient sein Geld mit Werbung. Mit dem Slogan, „Facebook ermöglicht es dir, mit den Menschen in deinem Leben in Verbindung zu treten und Inhalte mit diesen zu teilen", bewirbt das Unternehmen auf seiner Startseite seine kostenlose Plattform. Das Prinzip, alle Freundinnen und Freunde, Schulkameradinnen und -kameraden und auch alle Verwandten und Bekannten virtuell zu finden und zu binden und bei Bedarf jederzeit live, wechselseitig und interaktiv virtuell am Alltag teilzunehmen, bedurfte in unserer Medienwelt kaum einer Überzeugungskampagne. Besonders die jungen Generationen halten inzwischen den Verzicht auf eine mehrmalige tägliche Nutzung der Plattform für eine Zumutung. Studien[2] belegen, dass Jugendliche diese Art der Kommunikation für unentbehrlich halten. Bisweilen sehen Psychologen schon einen Suchtfaktor in verschiedenen Ausprägungsstufen.[3] Facebook weiß nicht nur sehr genau um diesen Umstand, sondern bekennt sich auch zum kulturellen Umbruch und treibt die Entwicklung immer weiter voran. Alles zu teilen, was bei herkömmlich analogem sozialen Umgang flüchtig ist und dem Vergessen anheim fällt, ist sogar das Credo von Facebook. Der Balanceakt zwischen Teilhabe, Öffnung der Privatsphäre oder gar informationellem Exhibitionismus einerseits und andererseits dem Urbedürfnis, die Kontrolle über Privates zu behalten und auf die Vergesslichkeit der Öffentlichkeit bei Bekanntgewordenem hoffen zu können, will

1 Dem Geschäftsbericht von Facebook zufolge sind Ende Dezember 2012 weltweit mehr als 1,06 Mrd. Nutzer aktiv, das wären rund 12 % der Weltbevölkerung. Davon entfallen etwa 24 Mio. auf Deutschland. Quellen: facebook Geschäftsbericht 2012 http://investor.fb.com/releasedetail.cfm?ReleaseID=736911 und SocialMediaSchweiz http://www.socialmediaschweiz.ch/html/infografik.html

2 „24 Hours: Unplugged", Studie der Universität of Maryland 21.4.2010 http://www.newsdesk.umd.edu/undergradexp/release.cfm?ArticleID=2144

3 Forscherteams um den Psychologen Assist. Prof. Wilhelm Hofmann (Booth School of Business der Universität Chicago Universität Chicago) fanden bei Probanden in einer Studie 2012 in Würzburg heraus, dass die höchsten Raten mangelnder Selbstkontrolle im Umgang mit sozialen Netzwerken zu beobachten waren. Quelle: http://news.uchicago.edu/article/2012/01/27/study-finds-lure-entertainment-work-hard-people-resist



inzwischen nicht mehr recht gelingen. Vor Jahren gepostete Fotos oder unbedachte Kommentare können eines Tages bei einem Bewerbungsgespräch zum Verhängnis werden. Seit 2004 entsteht unentwegt ein immer größer werdender Datenschatz. Der Wert dieses Schatzes entpuppt sich aber bei näherer Betrachtung weniger als der des Nutzers, als vielmehr der des Betreibers und seines Geschäftsmodells, mit der großen Datenmenge Werbeeinnahmen zu generieren. Und spätestens hier ruft man sich die Erkenntnis in Erinnerung, dass bei einem Produkt, das gratis angeboten wird, der Kunde selbst das Produkt ist.

Das Netzwerk haben wir – jetzt fehlt nur noch das Soziale

Zwar hat das Unternehmen in einigen Funktionsbereichen die Kontrollmöglichkeiten der Nutzer marginal weiterentwickelt und bietet etwa die Einstellbarkeit zur Sichtbarkeit bestimmter Angaben gegen andere Nutzer mit der Option zur Einschränkung an. Facebook stehen jedoch alle Daten uneingeschränkt zur Verfügung. Mit den „Datenverwendungsrichtlinien“, wie die Nutzungsbedingungen bei Facebook lauten, hat sich der Anbieter durch jeden Profilinhaber die schrankenlose Nutzung zusichern lassen. Die „Zusicherung“ ist jedoch nach den Maßstäben des in Deutschland gültigen Telemediengesetzes keine qualifizierte informierte Einwilligung, weil Umfang und Art der Präsentation der Nutzungsbedingungen keine eindeutige Kenntnisnahme sichert. Eine weitere Problematik stellt der Umfang und die Qualität der Daten dar, die sich Facebook zur freien Nutzung einräumen lässt.

Die Zusicherung der schrankenlosen Nutzung durch jeden Profilinhaber ist jedoch nach dem Telemediengesetz keine qualifizierte informierte Einwilligung.

Facebook-Fahndung: Alle Daten auf US-Servern

Die Polizeidirektion (PD) Hannover rief 2011 als Pilotprojekt (Modellversuch) die Fahndungsmitwirkung durch die Facebook-Gemeinde ins Leben. Hinweise aus der Bevölkerung zu erlangen, wie man es aus der Fernsehserie Aktenzeichen XY kannte, sollte auch unter Einbeziehung junger Generationen gelingen, die sich erfahrungsgemäß derartigen TV-Sendungen verweigern. Der Einrichtung einer Fanpage folgten starke Nutzerzahlenzuwächse. Aus den Anfängen einer Erprobung ergab sich eine Ausweitung und der Echtbetrieb. Im Sommer 2011 trat ich in eine Prüfung des Projektes ein. In der ersten Bewertung erläuterte das Niedersächsische Ministerium für Inneres und Sport (MI), dass die PD Hannover während der Pilotphase in erster Linie die Tauglichkeit einer Facebook-Fanpage für Maßnahmen der Öffentlichkeitsfahndung sowie der polizeilichen Öffentlichkeitsarbeit erprobt habe. Als „grundsätzlich gut leistbar" seien die Einrichtung und der Betrieb dieser Facebook-Präsenz beschrieben worden, der Nutzen sei „überaus gut".
Meine weiteren Nachfragen im November 2011 zielten auf die Rechtsgrundlage, die diesem hoheitlichen Handeln zwingend zugrunde liegen muss. Ich interessierte mich für zwei Varianten, die in Frage kamen:

- Lässt die PD Hannover die Datenverarbeitung gemäß § 6 NDSG in ihrem Auftrag durch Facebook durchführen? Dies wäre keine Datenübermittlung an Facebook, jedoch wäre dann ein schriftlicher Auftrag zwischen der Polizeidirektion Hannover als Auftraggeber und Facebook als Auftragnehmer abzuschließen (Auftragsdatenverarbeitung gemäß § 6 Abs. 3 S. 2 NDSG).
- Oder hat die PD Hannover Facebook im Rahmen einer Aufgabenübertragung (sog. Funktionsübertragung) eigentlich ihr obliegende Aufgaben/Funktionen (z.B. des Speicherns) übertragen? In diesem Fall liegt beim Einstellen von Daten auf der Kommunikationsplattform von Facebook durch die PD Hannover datenschutzrechtlich eine Datenübermittlung vor, die einer Rechtsgrundlage bedarf.

Betrieb der Fanpage kurzfristig eingestellt

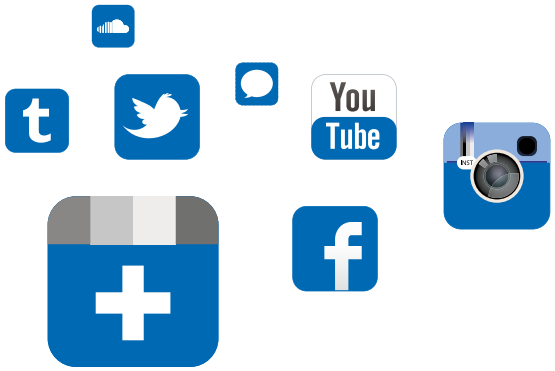
Mit dem MI wurde die rechtliche Zulässigkeit dieser Plattform am 20.1.2012 weiter erörtert. Meine Hinweise, dass nach der Strafprozessordnung (StPO) und den Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV) eine Öffentlichkeitsfahndung rechtlich nicht abgedeckt ist und es damit an einer normenklaren strafprozessrechtlichen und telemedienrechtlichen Ermächtigungsgrundlage fehlt, führte dazu, dass das Innenministerium zunächst die Fortsetzung des Fanpagebetriebes einstellte. Im März 2012 verfügte der niedersächsische Innenminister jedoch die Fortsetzung in modifizierter Form. In einer Pressemitteilung vom 6.2.2012 wurde dies mit dem Nutzwert begründet: Die bisherigen Erfolge belegten eindeutig, dass sich die Polizei diesem Medium nicht verschließen dürfe. Künftig sollten zunächst die Maßnahmen zur Öffentlichkeitsfahndung und Vermisstensuche über die Fanpage der Polizeidirektion Hannover zentral gesteuert werden. Im zweiten Schritt

sei, einhergehend mit einem neuen Internetauftritt der Polizei, ein zentraler Auftritt bei Facebook für alle Polizeidirektionen in Niedersachsen beim Landeskriminalamt geplant. Neu an dieser Konzeption war, dass künftig die im Zusammenhang mit Fahndungen und Vermisstensuche eingestellten personenbezogenen Daten auf polizeieigenen Servern gespeichert werden sollten. Zu den Fahndungs- und Suchhinweisen sollte der Besucher dann über einen Link auf der Polizei-Fanpage bei Facebook auf die polizeieigenen Server weitergeleitet werden. Auf der Fanpage sollte also nur noch ein Einstiegstext mit allgemeinen Hinweisen ohne personenbezogene Daten gepostet werden. Damit bliebe die Hoheit über die personenbezogenen Daten, besonders in Bezug auf die Speicherung und Löschung, bei der Polizei. Eine Übermittlung von personenbezogenen Daten in die USA sei somit nicht gegeben, damit fänden auch die datenschutzrechtlichen Belange Beachtung.
Bezogen auf die Inhaltsdaten der Postings traf dies nach meiner Auffassung tatsächlich zu. Was jedoch weiter außer Acht gelassen wurde, war die Verarbeitung personenbezogener Daten der Nutzer durch Facebook, die mit dem Besuch der Fanpage weiterhin erfolgte.

Intensive telemedienrechtliche Beratung für die Polizei verlief im Sande

In einer Stellungnahme vom 15. Mai 2012 zu einem „Richtlinien-Entwurf des Landeskriminalamtes Niedersachsen zur Öffentlichkeitsfahndung in Sozialen Netzwerken" erläuterte ich erneut die rechtlichen Bedenken und wies auf die Entschließung „Datenschutz bei sozialen Netzwerken jetzt verwirklichen!" der 82. DSB-Konferenz in München vom 28./29. September 2011 hin (www.datenschutz-bayern.de/dsbk-ent/DSK_82-Nutzerdaten.html). Danach bleiben die Gesetzgeber weiterhin aufgefordert, die Bestimmungen zur Öffentlichkeitsfahndung in der Strafprozessordnung und in den Polizeigesetzen (in Niedersachsen § 44 Abs. 2 Nds. SOG) mit Blick auf die technischen Weiterentwicklungen der Internetgesellschaft fortzuentwickeln und ggf. an die aktuellen Gegebenheiten anzupassen, und zwar normenklar und unter Einhaltung der Rechteabwägung zwischen Grundrechten der von dem Verfahren Betroffenen einerseits und dem Interesse der Strafverfolgung und der Gefahrenabwehr andererseits. Grund ist, dass die aktuell geltenden Vorschriften zu einer Zeit entstanden sind, als die Öffentlichkeitsfahndung per Internet mit all den sich hieraus ergebenden Problemen wie zum Beispiel der faktischen Unmöglichkeit, Daten im Netz wirkungsvoll zu löschen, noch nicht im gesetzgeberischen Blickfeld stand.
Nach dem Richtlinien-Entwurf des Landeskriminalamts sollten Fahndungsinhalte ausschließlich auf polizeieigenen Servern und polizeieigenen Internetseiten veröffentlicht werden, die Nutzung der Fanpages sollte gleichwohl fortgesetzt werden, eingeschränkt nur insofern, als nur noch anonymisierte Kurzhinweise auf die Fahndung mit einem Link auf die Fahndungsseite der Polizei gesetzt werden sollen.
Aufgrund dieser Aufteilung entfällt die Problematik der fehlenden normenklaren Ermächtigungsgrundlage zum Hosten der Daten bei einem Diensteanbieter außer-

Entschließungen der Konferenz der Datenschutzbeauftragten: www.lfd.niedersachsen.de >Allgemein >DSB-Konferenzen >Entschließungen



halb unseres gesetzlichen Geltungsbereiches zwar, jedoch waren aus telemedienrechtlicher Sicht Bedenken geblieben. Zu Recht weist der Richtlinien-Entwurf bei der Nutzung von sozialen Netzwerken darauf hin „dass es sich um ein Internetportal handelt, das von der im Privatbesitz befindlichen Fa. Facebook Inc. mit Sitz in den USA betrieben wird. So werden Daten, die auf Facebook-Fanpages veröffentlicht (gepostet) werden, nach derzeitigem Stand automatisch und ausschließlich auf Servern in den Vereinigten Staaten von Amerika gespeichert und weiterverarbeitet."

In Anbetracht der von deutschen und einigen anderen europäischen Datenschutzaufsichtsbehörden thematisierten materiellrechtlichen und technisch-organisatorischen Problemen bei der Nutzung der Social-Media-Dienste von Telemedienanbietern außerhalb der EU (namentlich insbesondere die bedeutendsten Dienste Facebook und Google+) halte ich es für geboten, auf die datenschutzrechtlichen Probleme im Zusammenhang mit den Nutzerdaten hinzuweisen. Denn neben der Problematik, die sich im Zuge der Veröffentlichung von Informationen über Personen, nach denen als Zeugen, mutmaßlichen Tätern oder Vermissten gesucht wird, ergibt, ist zusätzlich die telemedienrechtliche Verarbeitung von personenbezogenen Daten der Nutzer, die die Fanpage besuchen, und deren Recht auf informationelle Selbstbestimmung zu betrachten. In der rechtlichen Würdigung des Richtlinien-Entwurfes fehlten die Ergebnisse einer Prüfung und die Nennung konkreter Verstöße gegen europäisches, deutsches und niedersächsisches Datenschutzrecht, die einige Funktionen und die Datenverarbeitungsprozesse von Anbietern mit Sitz außerhalb der Europäischen Union beinhalten, weil diese Tracking- und Profiling-Funktionen der Nutzerdaten und Verkehrsdaten der Nutzer umfassen. Entscheidend ist, dass bei der Nutzung des Internets auf verschiedenen Ebenen die Persönlichkeitsrechte der Betroffenen und Nutzer zu beachten sind.

Vor allem die Suche von Zeugen im Wege der Öffentlichkeitsfahndung mittels Internet ist ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen. Die Nutzung des Internets zu diesem Zweck ist daher restriktiv zu handhaben. Denn neben der weltweiten Verfügbarkeit und der besseren Auffindbarkeit der Informationen, zum Beispiel von Bilddaten aufgrund innovativer Suchtechnologien, etwa der Gesichtserkennung, verliert die veröffentlichende Stelle mit der Übermittlung der Daten in das Internet die Kontrolle über den Umfang der Nutzung und Weiterverarbeitung der veröffentlichten Angaben. § 131 ff StPO und die Richtlinie über die Inanspruchnahme von Publikationsorganen und die Nutzung des Internets sowie anderer elektronischer Kommunikationsmittel zur Öffentlichkeitsfahndung nach Personen im Rahmen von Strafverfahren (Anlage B zur RiStBV) verfolgen daher bei der Nutzung

des Internets ein restriktives Konzept. Dieses ist auch und gerade bei der Nutzung des Dienstes Facebook zu beachten.

Digitale Tätowierung durch Internet-Fahndung

Die Bestimmungen zur Öffentlichkeitsfahndung nach §§ 131 bis 131c StPO in Verbindung mit der Anlage B der RiStBV und § 44 Nds. SOG stammen in ihrem Ursprung noch aus der „analogen" Zeit, in der mit Steckbriefen und anderen Plakaten oder in Zeitungen nach Verdächtigen gefahndet oder vor Gefahren gewarnt wurde. Sie wurden regional begrenzt veröffentlicht und nach ihrer Erledigung praktisch „rückstandsfrei gelöscht". Auch die Fahndung im Fernsehen (z.B. Aktenzeichen XY ungelöst) blieb in ihrer Wirkung auf einen relativ kurzen Zeitraum beschränkt. All dieses ist bei einer Fahndung im Internet allerdings nicht gewährleistet.

Zwar hat der Gesetzgeber versucht, die Internetfahndung in den zuvor genannten Vorschriften nur in relativ eng umgrenzten Fällen zuzulassen, dennoch bleiben die besonderen Gefahren des Internets bestehen. Der häufig zitierte Spruch „Das Internet vergisst nichts" bewahrheitet sich gerade in diesem Bereich immer wieder, da das Kopieren und Speichern derartiger Fahndungsaufrufe in der digitalen Welt keinerlei Probleme bereitet oder besondere Kosten entstehen lässt. Auch die Tatsache, dass die Fahndungsmeldungen nicht nur im räumlichen Bezug zu der Tat oder der Gefahr, sondern weltweit abrufbar sind – auch in Staaten, deren Datenschutzniveau das Unsere bei weitem nicht erreicht –, stellt eine besondere Gefährdung des Rechts auf informationelle Selbstbestimmung dar.

Durch die Ausbreitung der Sozialen Netzwerke im Internet kam zudem eine weitere Gefahr – nicht nur für den Datenschutz, sondern für Leib und Leben – für die Personen hinzu, nach denen gefahndet wird. Als ein Beispiel unter vielen mag hier ein Fall aus Emden dienen: Im März 2012 kam in Emden ein elfjähriges Mädchen gewaltsam zu Tode. Ein 17-Jähriger geriet wegen des Sexualmordes in Verdacht und wurde festgenommen. Schnell stellte sich heraus, dass er mit der Tat nichts zu tun hatte und unschuldig war. In einem sozialen Netzwerk im Internet jedoch schaukelte sich die Stimmung auf. Hetz- und sogar Lynchjustiz-Aufrufe wurden verbreitet. In der Folge versammelten sich ca. 50 Personen vor dem Gebäude der Polizei, drohten mit seiner Erstürmung und forderten die „Herausgabe" des Festgenommenen. Zwar wurden in der Folge zwei Personen wegen des Aufrufs zu einer Straftat verurteilt, doch der Schaden für den Rechtsstaat und insbesondere der psychische Schaden für den zunächst verdächtigen 17-Jährigen lassen sich dadurch allerdings nicht ungeschehen machen.

Auch wenn sich später ihre Unschuld erweist, bleiben die Angeprangerten in der öffentlichen Wahrnehmung häufig weiterhin Täter. Die Betroffenen werden so ihr Leben lang „digital tätowiert". Das sollten insbesondere die Justizminister nicht übersehen und sich die Frage stellen, wie sich die Facebook-Fahndung mit dem Grundgedanken der Resozialisierung verträgt – eines der wichtigsten Ziele unseres Strafrechts.

Den Nutzer in die Falle gelockt

Zusätzlich sind bei Nutzung der Facebook-Fanpage zur Öffentlichkeitsfahndung weitere rechtliche Rahmenbedingungen und eine Reihe tatsächlich vorhandener Umstände des verfolgten Geschäftsmodells und der technischen Implementierung des Dienstes zu beachten. So können in Abhängigkeit von den individuellen Einstellungen des Fanpage-Betreibers die auf einer Fanpage bereitgestellten Angaben auch von nicht registrierten Nutzern von Facebook wahrgenommen werden. Im „Gegenzug" stellt Facebook dem Fanpage-Betreiber unter anderem eine qualifizierte Nutzungsstatistik zur Verfügung. Aus dieser geht hervor, wie viele neue und wiederkehrende Nutzer die Seite aufgerufen haben. Die Nutzergruppen werden nach Alter, Geschlecht und Wohnort selektiert. Der durch Facebook beworbene Vorteil der Fanpage soll sein, dass die zur Verfügung gestellten Inhalte von Nutzern der Seite „geteilt" werden. Die mit einem Nutzer verbundenen „Freunde" können dann sehen, welche Informationen der jeweilige Nutzer interessant findet. Dies soll zu dem sogenannten „viralen Effekt" bei der Verbreitung der Information führen. Dieses Prinzip will sich die Polizei zunutze machen.

Die Erstellung einer Fanpage auf der technischen Plattform des Unternehmens Facebook Inc. ist die Erbringung eines Dienstes im Sinne des § 2 Nr. 1 Telemediengesetz (TMG) und die jeweilige Polizeibehörde wäre Diensteanbieter im Sinne dieser Vorschrift. Telemediendiensteanbieter sind sämtliche natürliche und juristische Personen, die eigene oder fremde Telemedien zur Nutzung bereithalten. Der Begriff der Telemedien wird gemäß § 1 Abs. 1 TMG im Wege der negativen Abgrenzung definiert. Alle Informations- und Kommunikationsdienste, die nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind, fallen unter den Begriff des Telemediums (Telemediendienstes). Maßgeblich für die Einordnung einer Fanpage als Telemediendienst ist die Bereitstellung von Informationen. Sofern die Polizei Niedersachsen eine Fanpage bei Facebook einrichtet, wie im Fall der PD Hannover und später aller Polizeibehörden in Niedersachsen bereits geschehen, wären somit die Vorgaben des Telemediengesetzes einzuhalten (§ 1 Abs. 1 S. 2 TMG).

Wer ist für Fanpages verantwortlich?

Fraglich ist auch, für welche Informationen der Betreiber einer Fanpage die datenschutzrechtliche Verantwortung trägt. Zu unterscheiden ist hierbei zwischen der Verantwortung für den Umgang mit Inhaltsdaten sowie Bestands- und Nutzungsdaten (§§ 14 und 15 TMG). Rechtlich unbestritten ist die datenschutzrechtliche Verantwortung des Fanpage-Betreibers für die auf der Seite veröffentlichten Informationen, zumal er sie selbst redaktionell bestimmt und postet. Die Zulässigkeit der Veröffentlichung dieser Angaben bemisst sich nach den bereichsspezifischen Vorgaben zum Beispiel der StPO. In diesem Zusammenhang wies ich erneut auf §§ 131 ff StPO und Nr. 3.2 „Nutzung des Internets" der Anlage B zur RiStBV hin. Danach sollen private Internetanbieter bei der Fahndung „grundsätzlich nicht eingeschaltet werden". Eine Einbindung Facebooks würde gegen diese eindeutige Vorgabe verstoßen. Aus datenschutzrechtlicher Sicht unzulässig wäre außerdem die Weiterverwendung der auf der Fanpage eingestellten Informationen durch Facebook. Das Verhältnis zwischen dem für die Inhalte verantwortlichen Dienstanbieter und dem technischen Provi-

Nach der RiStBV sollen private Internetanbieter bei der Fahndung „grundsätzlich nicht eingeschaltet werden". Eine Einbindung Facebooks würde gegen diese eindeutige Vorgabe verstoßen.

der für die Zurverfügungstellung der Seite ist im Regelfall eine Auftragsdatenverarbeitung gemäß § 6 NDSG. Daraus folgt, dass der Auftragsdatenverarbeiter die Daten nur nach Weisung und nicht zu eigenen Geschäftszwecken erhebt, verarbeitet oder nutzt. Diese Bedingung erfüllt die Facebook Inc. jedoch nicht. In Ziffer 2.1 der Nutzungsbedingungen vom 4. Oktober 2010[4] lässt sich Facebook „eine nicht-exklusive, übertragbare, unterlizenzierbare, gebührenfreie, weltweite Lizenz für die Nutzung jeglicher IP-Inhalte" einräumen, die Nutzer auf Facebook veröffentlichen oder im Zusammenhang mit der Nutzung an Facebook übermitteln. Nach Angaben von Facebook endet die Lizenz, wenn der Nutzer die Inhalte oder das Konto löscht, es sei denn, die Inhalte wurden mit anderen Nutzern geteilt, und diese haben die Inhalte nicht gelöscht.

Nutzung von Facebook zur Öffentlichkeitsfahndung datenschutzrechtlich unzulässig

Aufgrund dieser Regelung ist das Verhältnis zwischen der Polizei und Facebook keine Auftragsdatenverarbeitung. Denn es muss davon ausgegangen werden, dass Facebook die durch die Polizei eingestellten Inhalte auch zu eigenen Zwecken nutzt. Daher ist die Veröffentlichung der Daten auf einer Fanpage auch eine Datenübermittlung an Facebook mit Sitz in den USA. Nach meiner Rechtsauffassung beinhalten die §§ 131–132 StPO keine Rechtsgrundlage für die Übermittlung der Daten in das außereuropäische Ausland.
Ergänzend sehe ich die schutzwürdigen Interessen der Betroffenen, insbesondere die der Zeugen, verletzt, wenn deren Daten in die USA übermittelt werden, ohne dass die Polizei in der Lage wäre, effektiv die Kontrolle über den Umgang mit den Daten auszuüben. Daraus folgt, dass damit die Nutzung des Dienstes Facebook zur Öffentlichkeitsfahndung datenschutzrechtlich unzulässig ist.

Ist Reichweitenanalyse zulässig? Wer steht datenschutzrechtlich in der Verantwortung?

Umstritten ist, ob Fanpage-Betreiber auch für die bei der Nutzung der Fanpages betriebene Reichweitenanalyse datenschutzrechtlich verantwortlich sind. Facebook betreibt einen Webanalysedienst namens „Facebook Insight"[5] im Zusammenhang mit dem Betrieb des Sozialen Netzwerkes. Dieser Dienst setzt Cookies bei sämtlichen Nutzern, die mit der Domain facebook.com interagieren. Nach Kenntnis der deutschen Datenschutzbehörden[6] werden bei angemeldeten Nutzern die Cookies zur Analyse ihres Nutzungsverhaltens eingesetzt, um auf diese Weise Aufschluss über die Interessen, Vorlieben und Neigungen der Nutzer zu gewinnen. Zu diesem Zweck reichert Facebook das Profil der Nutzer mit deren Nutzungsdaten an. Diese Daten werden dann von Facebook zu Werbezwecken verwendet. Außerdem erstellt Facebook auf der Grundlage dieser Daten Fanpage-Betreibern eine

4 http://www.facebook.com/legal/terms?locale=de_DE
5 http://www.facebook.com/legal/terms?locale=de_DE
6 Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSB-K) steht unmittelbar und mittels Fachar beitskreise im fachlichen Austausch. Die für Facebook zuständige Aufsichtsbehörde ist, sofern der Firmensitz der Niederlassung „Facebook Germany GmbH" Hamburg betroffen ist, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI)

Nutzungsstatistik über die Art und den Umfang der Nutzung der Seite. Gemäß § 15 Abs. 3 TMG dürfen Diensteanbieter Nutzungsdaten zum Zweck der Reichweitenanalyse verwenden. Voraussetzung ist, dass

- die Profile nur einem Pseudonym zugeordnet sind,
- die Nutzer über den Umstand der Reichweitenanalyse sowie deren Umfang informiert werden,
- die Nutzer die Möglichkeit des Widerspruches haben und
- die erstellten Nutzungsprofile nicht mit identifizierenden Angaben des jeweiligen Nutzers zusammengeführt werden (§ 15 Abs. 3 Satz 3 TMG). Die Missachtung des Trennungsgebotes stellt einen Bußgeldtatbestand gemäß § 16 Abs. 2 Nr. 5 TMG dar.

Keine der Anforderungen des § 15 Abs. 3 TMG wird von den Fanpage-Betreibern oder von Facebook erfüllt. Weder erfolgt eine ausreichende Information, noch können Nutzer gegen die Erfassung des Nutzungsverhaltens Widerspruch einlegen. Außerdem beachtet Facebook das Trennungsgebot nicht. Denn die unter Pseudonym mittels Cookies gesammelten Daten werden mit dem individuellen Profil des Nutzers zusammengeführt. Damit missachtet Facebook das gesetzliche Ziel, die Reichweitenanalyse nur zuzulassen, wenn der jeweilige Nutzer nicht identifiziert wird. Facebook verstößt gegen diese gesetzlichen Vorgaben, indem es die individuellen Nutzungsgewohnheiten der angemeldeten Nutzer erfasst und auswertet. Nach einhelliger Auffassung der Aufsichtsbehörden des Bundes und der Länder verwirklicht Facebook damit den Bußgeldtatbestand des § 16 Abs. 2 Nr. 5 TMG. Eine diese Reichweitenanalyse rechtfertigende Einwilligung der Nutzer im Sinne des Niedersächsischen Datenschutzgesetzes (NDSG) sowie des TMG liegen nicht vor.

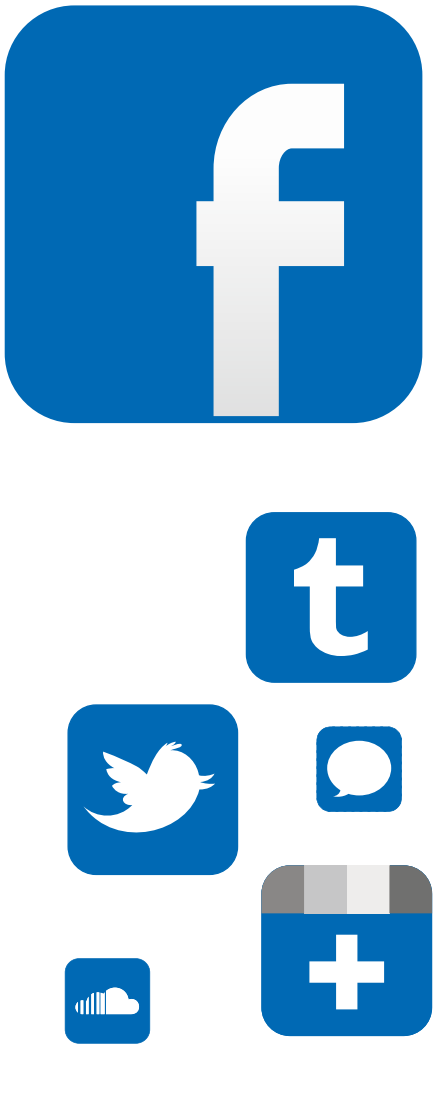
Fraglich ist jedoch, ob dieser Verstoß den Fanpage-Betreibern zugerechnet werden kann. Nach Auffassung der Datenschutzbehörden spricht derzeit vieles zugunsten einer Verantwortlichkeit der Fanpage-Betreiber, da diese durch die Einrichtung einer Fanpage erst den Anlass für die Erstellung der Nutzungsprofile geben. Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat als für das Land Schleswig-Holstein zuständige Aufsichtsbehörde bereits einzelnen Fanpage-Betreibern die Nutzung des Dienstes Facebook im Wege der verwaltungsrechtlichen Anordnung untersagt. In dem vom ULD geführten Musterprozess vor dem zuständigen Verwaltungsgericht in Schleswig, bei dem es um die Frage der datenschutzrechtlichen Verantwortung für die Durchführung der Reichweitenanalyse gehen sollte, kam es zu keiner inhaltlichen Entscheidung, weil das Gericht die Zuständigkeit für die Aufsicht der irischen Datenschutzaufsicht zuschrieb.

Sollte sich herausstellen, dass die Polizei für die von Facebook betriebene Reichweitenanalyse datenschutzrechtlich verantwortlich ist, hätte sie den Bußgeldtatbestand des § 16 Abs. 2 Nr. 5 TMG verwirklicht.

Im Ergebnis vertrat ich gegenüber der Polizei Niedersachsen die Auffassung, dass eine Nutzung der Fanpages des Dienstes Facebook unter den derzeitigen tatsächlichen Gegebenheiten zum Zweck der Fahndung datenschutzrechtlich nicht vertretbar wäre. Sollte sich im Nachhinein herausstellen, dass die Polizei für die von Facebook betriebene Reichweitenanalyse datenschutzrechtlich verantwortlich ist, hätte dies zur Folge, dass die Polizei den Bußgeldtatbestand des § 16 Abs. 2 Nr. 5 TMG verwirklicht hätte. Selbst wenn eine unmittelbare datenschutzrechtliche Verantwortung nicht festgestellt würde, erschiene es jedoch als rechtspolitisch absolut fragwürdig, wenn die Polizei einen Dienst für die Strafverfolgung nutzte, der, wäre

der Betreiber in Deutschland ansässig, nach deutscher Gesetzeslage unzweifelhaft unzulässig wäre.

Facebook-Fahndung mittels Verlinkung auf Polizei-Server



Die geplante Variante in Niedersachsen, auf den Fanpages lediglich Links mit Verweis auf die eigentlichen Fahndungen auf den Servern der Polizei bzw. deren originären Providern zu veröffentlichen, wurde von der Richtlinie des Landeskriminalamtes Niedersachsen favorisiert. Damit entfällt die zuvor beschriebene Problematik. Jedoch bleibt es in dieser Konstellation bei der beschriebenen Verantwortlichkeit für die Reichweitenanalyse. Die PD Hannover forderte inzwischen (Mai 2012) die Nutzer nach meinen Feststellungen in zahlreichen Postings mit dem folgenden Text auf, sichere Rückkanäle zu nutzen: „Hinweise bitte NUR an die Polizeidienststelle xy 0511 109-xxxx und NICHT über die Kommentarfunktion." Dieser Hinweis stellt beim Betrieb der Fanpage jedoch die einzige der Polizei zur Verfügung stehende Steuerungsmöglichkeit dar, dem im Interesse der Nutzer zu beachtenden Datensparsamkeitsprinzip zu folgen. Die Auswirkung erreicht jedoch nicht den nach deutschem Datenschutzrecht zu fordernden Grad des Schutzes. Da das Partizipationsprinzip in sozialen Netzen systemimmanent ist, bleibt es bei der Verarbeitung der personenbezogenen Verkehrsdaten und Nutzungsdaten im Sinne des TMG, die zu überschüssigen Daten bei Facebook führen. Ferner bleibt es zudem bei der aktiven Ermutigung zum Besuch der Fanpage seitens eines Hoheitsträgers, die rechtlich nicht haltbar ist.

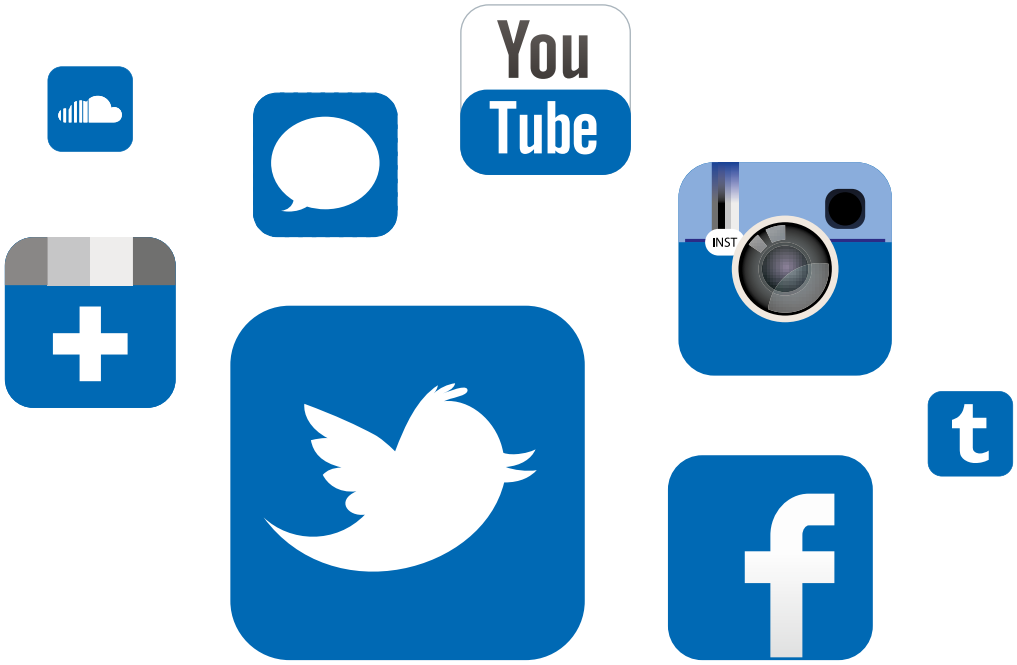
Bundesweite Abstimmungen

Der IT-Planungsrat Bund/Länder fasste in seiner Sitzung am 8.3.2012 zum Thema „Soziale Netzwerke und Datenschutz" den folgenden Beschluss:

1. Der IT-Planungsrat nimmt den Bericht der Datenschutzvertreter zum Datenschutz in Sozialen Netzwerken zur Kenntnis und begrüßt die Initiative des Bundes, eine entsprechende Selbstregulierung herbeizuführen.
2. Der IT-Planungsrat empfiehlt den öffentlichen Stellen des Bundes und der Länder, insbesondere vor der direkten Einbindung von Social-Plugins und bei der Nutzung von Fan-Pages eine sorgfältige Prüfung unter Einbeziehung der Datenschutzbeauftragten vorzunehmen.

Bei der Umsetzung der geplanten Richtlinie für die Polizei Niedersachsen empfahl ich dem Innenministerium daher, der Nutzerdatenproblematik eine besondere Bedeutung zukommen zu lassen. Abschließend verwies ich darauf, dass sich der Arbeitskreis I der Innenministerkonferenz mit dem Thema ausführlich befasst hatte und bat um zeitnahe Mitteilung des Sachstandes der Beratungen und die Auswirkungen auf die Planungen für den Polizeibereich. Leider ist diese Information bis zum Ende des Berichtszeitraumes nicht erfolgt.

Wie sich herausstellte, lag der „Ergebnisbericht der Arbeitsgruppe des AK I ‚Staatsrecht und Verwaltung' zum Datenschutz in Sozialen Netzwerken"[7] seit dem 4. April 2012 vor, war aber erst im Herbst freigegeben und zugänglich gemacht worden. Er nimmt ebenfalls inhaltlich sehr kritisch Stellung, schließt jedoch die Nutzung von Facebook nicht kategorisch aus. Leider wurden auch – ungeachtet der massiven Einwände gegen das Projekt – Fakten geschaffen: Mit Runderlass vom 7. Juni 2012 erließ das Innenministerium gleichwohl die verpflichtende Regelung für die sechs niedersächsischen Polizeidirektionen, die Zentrale Polizeidirektion, die Polizeiakademie und das Landeskriminalamt, bei Facebook Fanpages einzurichten und die Fahndung in der vorgenannten modifizierten Form weiterzubetreiben.
Ich halte weiterhin den Betrieb aus den dargelegten Gründen für telemedienrechtlich unzulässig.



Keine Einigung beim Social-Media-Leitfaden des MI für die niedersächsische Landesverwaltung

Angesichts der öffentlichen Diskussion und fachlichen Diskurse, ob die Nutzung von Fanpages für den öffentlichen Bereich zulässig und vertretbar sei, entstand in der Landesverwaltung zunehmend der Bedarf nach einer Regelung, wie mit den Medien des sogenannten Web 2.0, den Social-Media-Plattformen, umzugehen sei.
Der Niedersächsische IT-Planungsrat als strategisches Entscheidungsgremium der Landesregierung für Niedersachsen, beauftragte daher das Innenministerium, einen Leitfaden zu erstellen. Der Entwurf für den „Behörden-Leitfaden: Umgang mit webbasierten sozialen

7 Veröffentlicht auf der Seite des ULD https://www.datenschutzzentrum.de/internet/20120404-AG-SozNetzw-AK-I-IMK.pdf

Medien (Social Media)“ wurde mir vorgelegt. In einer umfangreichen schriftlichen Stellungnahme (mit drei Durchläufen vom 30.4.12, 11./14.5.2012 und 29.6.2012) sowie einer Erörterung im IT-Planungsrat legte ich dar, dass ein Leitfaden nicht nur die Nutzenpotentiale hervorheben und ansonsten, wie geschehen, lediglich von einigen Risiken ausgehen sollte, da es zudem tatsächlich eine ganze Reihe von Mängeln einiger Funktionen und Datenverarbeitungsprozesse gebe, die gegen europäische, deutsche und niedersächsische datenschutzrechtliche Bestimmungen verstießen.

So wurde unter anderem vorgeschlagen, die positiven Nutzen wie folgt zu ergänzen: „Die Nutzung von Social Media bietet für die öffentliche Verwaltung interessante Chancen zur Verbesserung der Arbeitserledigung. Sie birgt aber auch zahlreiche Risiken und zieht in bestimmten Konstellationen sogar rechtswidriges Verwaltungshandeln nach sich. Dieser Leitfaden geht auf alle drei Dimensionen – Chancen, Risiken und Rechtsrahmen – ein, Schwerpunkt des Leitfadens ist jedoch, auf Gefahren und rechtliche Regelungen hinzuweisen und Maßnahmen zur Abwehr dieser Gefahren und zur Vermeidung von Rechtsverstößen zu beschreiben – um so das Risiko bei der Nutzung von Social Media in der öffentlichen Verwaltung zu minimieren.“

Dabei wurden von mir die Aspekte nicht nur theoretisch benannt, sondern eine vollständige Überarbeitungsfassung zu dem Leitfaden geliefert. Ich verband dies mit dem Angebot, bei vollständiger Übernahme meiner Ergänzungs- und Änderungsempfehlungen in der letzten Fassung, oder ggf. abgestimmten Modifikationen im Anschluss, die Mitwirkung des LfD NI an dem Leitfaden im Impressum zu dokumentieren, um Zweifeln an der Datenschutzkonformität zu begegnen.

Den Änderungsvorschlägen wollten das Innenministerium und der IT-Planungsrat jedoch nicht vollständig folgen. Der Umlaufbeschluss dazu kam am 10.9.2012 zustande.[8] Insbesondere die potentielle Rechtswidrigkeit und die Hinweise, wie diese zu verhindern sind, wird nun im Leitfaden nicht genannt. Im Ergebnis ist zu konstatieren, dass der Aussagewert des Leitfadens damit deutliche Einbußen erlitten hat, weil die Leser hinsichtlich der rechtlichen Fallstricke nicht ausreichend auf die Materie vorbereitet werden.

Viele Kommunen wollen Fanpage: Zwischen Medienhype und rechtlicher Verunsicherung

Im Berichtszeitraum erreichten mich vermehrt Anfragen zur Rechtmäßigkeit der Nutzung von Social-Media-Plattformen durch öffentliche Stellen. Insbesondere bei Kommunen war und ist ein steigender Trend zu beobachten, bei Facebook eine Fanpage einzurichten. Die Anfragen zeigten, dass die Kenntnisse über technische und rechtliche Zusammenhänge in einigen Fällen sehr lückenhaft waren. Aufgrund des offenkundigen erheblichen Bedarfs an Aufklärung war das Engagement meiner Behörde zum Thema Social Media gefordert. Im Jahre 2012 engagierte sich mein

8 Bekanntmachung d. MI v. 18.10.2012 -42.02840/1100-0003-: Umgang mit webbasierten sozialen Medien (Social Media), Nds. MBl. Nr. 39/2012 v. 7.11.2012, S. 885 ff; http://www.niedersachsen.de/download/72465/Nds._MBl._Nr._39_2012_vom_07.11.2012_S._885-928.pdf

Technikreferat daher verstärkt bei mehreren Tagungen der kommunalen Spitzenverbände und Behörden mit Vorträgen zur Darstellung der technischen und rechtlichen Zusammenhänge und der Risiken. Wichtig war hierbei auch, die konkreten Rechtsverstöße nach deutschem und europäischem Datenschutzrecht herauszuarbeiten. Nach meiner Auffassung obliegt den öffentlichen Stellen zuvorderst die Pflicht zur Rechtmäßigkeit des Verwaltungshandelns im Rahmen des Rechtsstaatsprinzips. Jedoch ist spürbar, dass die Kommunen dem allgemeinen Trend unterliegen und der Erreichbarkeit der jungen Generationen große Bedeutung zumessen. Meines Erachtens darf dabei in der Abwägung die Frage der Rechtmäßigkeit nicht ins Hintertreffen geraten.

Präventionsangebote: DsIN-Schulungen

Aus den Erfahrungen der Beratungs- und Aufsichtstätigkeit ergab sich die Erkenntnis, im Datenschutzinstitut (DsIN) ein Fortbildungsangebot zu entwickeln, um öffentlichen Stellen systematisch die für dieses Rechtsgebiet notwendigen Kenntnisse zu vermitteln. Die Konzeptionsphase lief im Herbst 2012 an. Im Mai 2013 wurde das erste von mehreren für das Jahr 2013 geplanten Seminare durchgeführt.

Arbeitshilfe des DStGB zu unkritisch

Der Niedersächsische Städte- und Gemeindebund brachte am 14.9.2012 eine Arbeitshilfe „Städte und Gemeinden in sozialen Netzwerken“[9] heraus. Sie ist in einer übergreifenden Kooperation des Deutschen Städte- und Gemeindebundes mit dem Niedersächsischen Städte- und Gemeindebund, der Kommunaltreuhand Deutschland und unter Mitwirkung zahlreicher Praktiker entstanden. Ich hätte es begrüßt, wenn die Bewertung neben der Darstellung der Vorteile der in Frage stehenden Social-Media-Plattformen angesichts der bestehenden datenschutzrechtlichen Probleme kritischer ausgefallen wäre.

Orientierungshilfe „Soziale Netzwerke“

Seit Sommer 2012 entwickelte der AK Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Orientierungshilfe „Soziale Netzwerke“. Im März 2013 wurde diese mit folgender Entschließung[10] angenommen und veröffentlicht:

9 Arbeitshilfe des NStGB: http://www.nsgb.de/magazin/artikel.php?artikel=1331&type=2&menuid=35&topmenu=35

10 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14.3.2013 http://www.datenschutz.bremen.de/sixcms/detail.php?gsid=bremen236.c.7669.de PDF downloaden: http://www.datenschutz.bremen.de/sixcms/media.php/13/Orientierungshilfe%20Soziale%20Netzwerke.pdf

„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. Sie soll die Betreiber sozialer Netzwerke und die die Netzwerke nutzenden öffentlichen und privaten Stellen bei der datenschutzgerechten Gestaltung und Nutzung der Angebote unterstützen. 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 erneut nachdrücklich hin."

Orientierungshilfe „Soziale Netzwerke": www.lfd.niedersachsen >Themen >Internet >Information für Webseitenbetreiber

Orientierungshilfe für Anbieter von Telemedien

Eine weitere grundlegende Orientierungshilfe befasst sich mit den Pflichten der Telemedienanbieter.[11] Neben der Definition (Diensteanbieter, Telemedien) und den von Diensteanbietern zu beachtenden Vorschriften werden die Grundlagen (Impressumspflicht, Links auf fremde Inhalte) erklärt. Schwerpunkt ist der Umgang mit personenbezogenen Daten und die Klärung, welche Daten dazugehören. Außerdem werden die Grundsätze zur Verarbeitung personenbezogener Daten dargelegt (Datengeheimnis, die Bestellung eines betrieblichen Datenschutzbeauftragten, die Verfahrensbeschreibung, die Auftragsdatenverarbeitung und die technischen und organisatorische Maßnahmen, einschließlich der Verschlüsselung).

Orientierungshilfe für Anbieter von Telemedien: www.lfd.niedersachsen.de >Themen >Internet >Information für Webseitenbetreiber

11 „Orientierungshilfe für Anbieter von Telemedien", Stand: 26.4.2013, http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=28288&article_id=98353

Soziale Netzwerke, Internetforen, Onlinehandel: Datendiebstähle nehmen zu

Wenn der frühere Chaos Computer Club (CCC)-Sprecher „Ron“ auf dem 28. Chaos Communication Congress (28C3) im Dezember 2011 in Berlin davon berichtete, dass „Datenwegkommnisse“ erwartungsgemäß zum „Grundrauschen“ geworden seien, dann fasst dies sehr prägnant zusammen, wie alltäglich kriminelle Angriffe auf die Privatsphäre geworden sind. Schon 2006 formulierte der Werbefachmann Michael Palmer die These: „Daten sind das neue Öl.“ Es ist also nicht verwunderlich, dass bei der Jagd nach diesem wertvollen Rohstoff alle Mittel ausgeschöpft werden. Soziale Medien, die ihre Nutzer als Ware vermarkten, bilden hier tatsächlich nur die Spitze des Eisbergs.

Wer versucht, sich von den Vermarktern der eigenen Nutzungsgewohnheiten fernzuhalten, muss immer öfter feststellen, dass auch personenbezogene Daten, die für den Onlinehandel notwendig sind, eine gefragte Ware darstellen. In Niedersachsen konnte ich eine signifikante Zunahme der Anzahl gehackter online verfügbarer Datenbanken registrieren, aus denen personenbezogene Daten für den Datenhandel abgezogen worden waren. Die Bandbreite der betroffenen Unternehmen reichte dabei vom kleinen spezialisierten Onlinefachhändler über den Schulbuchverlag bis zum großen Online-Versandhandel für Hardware, Software, Entertainment und Kommunikation. In einem Fall landeten schließlich über 190.000 Adresssätze mit Telefonnummer und E-Mail-Adressen für jedermann abrufbar bei einem Sharehoster. Einer Selbstbezichtigung des mutmaßlichen Täters zufolge erhielt er für die betroffenen Daten 250 Euro. Computerkriminelle bieten den Hack einer normalen Webseite nach 28C3-Angaben jedoch schon für 9,99 Dollar an, und die vollständige Kontrolle über einen Regierungswebserver kostet etwa 499 Dollar. Dagegen werden Kontozugangsdaten mit bis zu 700 Dollar pro Datensatz vergleichsweise teuer gehandelt.

Schwachstellen durch fehlende Abwehrsysteme

Ein Intrusion Detection System (IDS) ist ein Angrifferkennungssystem zur Erkennung von Verhaltensmustern, die als Angriffe gegen eine Datenverarbeitungsanlage bewertet werden.

Besondere Schwachstellen der betroffenen Internetangebote offenbarten sich im Bereich des technisch-organisatorischen Datenschutzes: Keines der Unternehmen verfügte über ein funktionierendes so genanntes Intrusion Detection System oder gar über ein Intrusion Prevention System. Daher wurden die meisten Fälle erst bekannt, als Kunden Spam-Mails auf E-Mail-Adressen erhielten, die exklusiv für die Kommunikation mit den betroffenen Unternehmen genutzt wurden.

Die Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten gemäß § 42a Bundesdatenschutzgesetz (BDSG) verpflichtet jedoch Unternehmen nur dann zu einer Information der Aufsichtsbehörde und der Betroffenen, wenn bei ihr gespeicherte

- besondere Arten personenbezogener Daten (§ 3 Absatz 9),
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten

Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.
Dies führte dazu, dass in einigen Fällen Unternehmen zunächst bemüht waren, den Vorfall zu verbergen und gar nicht auf die Auskunftsersuchen der betroffenen Kunden einzugehen. Diese wandten sich dann an die Aufsichtsbehörde. Da sich die Kunden häufig in Foren informieren, laufen Versuche, solche Vorfälle zu vertuschen, meist ins Leere und erzeugen erst recht eine ungewollte Aufmerksamkeit. Unternehmen, die solche Vorfälle ihren Kunden transparent machen und Mängel zeitnah abstellen, können dagegen viel eher mit einer positiveren Resonanz rechnen.

Als Intrusion Prevention System (IPS) wird ein IDS bezeichnet, das über die eine Generierung von Meldungen hinaus Funktionen bereitstellt, entdeckte Angriffe abwehren können.

Strafverfolgungsbehörden oft nicht eingeschaltet

Bei den im Berichtszeitraum von meiner Behörde untersuchten Fällen schalteten die Unternehmen häufig nicht die Strafverfolgungsbehörden ein. Daher gehe ich davon aus, dass es in der polizeilichen Kriminalstatistik im Bereich der Computerkriminalität eine hohe Dunkelziffer gibt. Die häufigsten Gründe hierfür waren, dass die Vorfälle nicht zeitnah festgestellt werden konnten oder Spuren ins Ausland führten und sich die betroffenen Unternehmen daher keine großen Erfolgsaussichten für eine strafrechtliche Verfolgung ausrechneten.
Wie auch im vergangenen Berichtszeitraum betraf 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 Zuständigkeit fielen. Neben den Diskussionen zu Fahndung, Klarnamenzwang und Gesichtserkennung über hochgeladene Fotos in den beiden großen amerikanischen sozialen Netzwerken gab es auch Positives aus den USA zu berichten. So ist nun ein beanstandungsfreier Betrieb von Google Analytics möglich, und die Gesichtserkennung in Facebook für Europa wurde abgeschaltet. Nutzer, die das Feature weiter verwenden wollen, müssen nun der Gesichtserkennung zuerst zustimmen.

Lieber sparen als schützen

Die Verarbeitung von personenbezogenen Daten im Internet für die soziale Interaktion oder den Onlinehandel ist alltäglich. Der technisch-organisatorische Schutz dieser Daten wird sowohl von den Nutzern, als auch den Anbietern regelmäßig vernachlässigt. Die Nutzer messen der Bequemlichkeit und den vermeintlichen Sparmöglichkeiten eine höhere Priorität bei als dem Schutz ihrer Privatsphäre. Viele folgen dem Mainstream nach dem Motto: Wenn alle das machen, dann kann es ja nicht verkehrt sein, und außerdem hab' ich ja nichts zu verbergen. Auch auf der Anbieterseite wird zu sehr auf diesen Mainstream vertraut. Softwarelösungen werden unreflektiert aus der USA übernommen, Gefährdungsanalysen nicht vorgenommen.
Wenn es um das „neue Öl" geht, dann sollten sowohl Nutzer als auch Anbieter darauf achten, dass dieses knappe Gut auch angemessen behandelt wird. Nutzer wie Anbieter von Telemedien müssen sich bewusst sein, dass Unternehmen mit Sitz außerhalb des Euro-

päischen Wirtschasftsraums (EWR) regelmäßig keinen angemessenen Datenschutzstandard aufweisen. Auch sollte klar sein, dass personenbezogene Daten durch angemessene technisch-organisatorische Maßnahmen geschützt werden müssen und dies Geld kostet.

Während ein echter Datengau bei einem Unternehmen „nur" zu Ansehensverlust und wirtschaftlichen Einbußen führen dürfte, so trifft es den Nutzer oft ungleich schwerer, wenn in seine Privatsphäre eingebrochen wird. Das tragische Schicksal von Amanda Todd steht beispielhaft für die möglichen Folgen, die drohen, wenn private Inhalte öffentlich werden. Die Kanadierin hatte sich als 12-Jährige in einem Chat per Webcam dazu überreden lassen, vor einem Fremden ihren Oberkörper zu entblößen. Mit einem Mitschnitt dieser Szene wurde sie von dem Fremden erpresst. Er veröffentlichte das Video im Internet, woraufhin das Mädchen in der Schule gemobbt wurde. Mehrere Schulwechsel und Umzüge der Familie blieben erfolglos, denn das Video wurde gezielt auch an den neuen Orten bekanntgemacht. Es folgten Selbstverletzungen und ein gescheiterter Suizidversuch. Im Alter von 15 Jahren erhängte sich Amanda schließlich. Vor ihrem Tod veröffentlichte sie ein neunminütiges Video, in dem sie über ihre Geschichte schweigend mit handgeschriebenen Zetteln berichtete.

Doch ist es inzwischen nicht mehr nötig, dass eine Person aktiv eine andere ausspäht, um an solche brisanten Daten zu kommen. Aktuelle Spyware und Malware wie Superclean oder DroidCleaner kompromittieren nicht nur die auf dem Smartphone gespeicherten Daten (hier werden zum Beispiel der Inhalt der Speicherkarte, alle SMS-Nachrichten und alle Kontaktdaten und Fotos kopiert und versendet), sondern bei Anschluss an einen PC auch diesen.

Datenschutzinstitut Niedersachsen: Schulungsbedarf durch IT-Innovationen weiter angestiegen

Wie in den vergangenen Jahren hat auch im Berichtszeitraum eine Reihe von Veranstaltungen im Datenschutzinstitut Niedersachsen (DsIN) stattgefunden. Als Erfolgsmodell hat sich dabei erneut die mehrtägige Seminarreihe „Basiswissen für behördliche Datenschutzbeauftragte" herausgestellt. In dieser aus vier Tagesseminaren bestehenden Veranstaltungsreihe werden die grundlegenden rechtlichen und technisch-organisatorischen Aspekte der Tätigkeit eines behördlichen Datenschutzbeauftragten dargestellt und an Hand praktischer Beispiele mit den Teilnehmern durchgespielt.

Der berechtigt hohe Anteil von zwei Seminartagen für den technisch-organisatorischen Teil erfordert bei jährlich vier bis fünf Veranstaltungen ein hohes Maß an personellem Aufwand und Einsatz. Darüber hinaus werden jährlich vier Einzelveranstaltungen aus dem technisch-organisatorischen Bereich angeboten. Wie sich in den zurückliegenden zwei Jahren gezeigt hat, ist das LfD-Technikreferat 3 damit allerdings auch an der Grenze der zeitlichen und personellen Möglichkeiten angelangt; eine weitere Intensivierung der Arbeit im Fortbildungsbereich ist ohne personelle Aufstockung nicht mehr leistbar. Bis zum Herbst 2012 wurden alle Angebote, die insgesamt 23 Nettoschulungstage umfassten, von zwei Mitarbeitern und dem Leiter des Referats 3 geleistet, parallel zu deren Aufgaben der Eingabenbearbeitung, Beratung und Kontrolle. Der Aufwand für Vor- und Nachbereitung dieser für den Datenschutz präventiven Aus- und Fortbildungsangebote schlägt je nach Veranstaltung und Thema zeitlich zusätzlich mit 80 bis 300 Prozent zusätzlich zu Buche, so dass insgesamt etwa 60 Personentage im Berichtszeitraum vom Technikreferat geleistet worden sind. 23 der 51 DsIN-Veranstaltungen (45 Prozent) wurden vom Technikreferat durchgeführt. Dies zeigt auch, wie sehr die IT – neben der juristischen Bewertung – die Datenschutzthemen inzwischen dominiert. Seit Ende 2012 steht ein weiterer Mitarbeiter für den Bereich des technisch-organisatorischen und materiellen Datenschutzes im Bereich Telemedien bereit. Er wird speziell in diesem Bereich ein weiteres Fortbildungsangebot im DsIN durchführen, das sich vorrangig mit Web 2.0 und den sozialen Netzwerken (Social Media) und deren besondere datenschutzrechtliche Herausforderungen befasst (vgl. Beitrag Social Media Seite 118).

Expertenkreis für IT-Führungskräfte: Beratung, Hilfe und Austausch für den öffentlichen Bereich

Zusätzlich zu den genannten Kursangeboten wurde die Reihe der Veranstaltungen des Gesprächs-/Expertenkreises im DsIN fortgesetzt. Im letzten Tätigkeitsbericht (für 2009–2010) hatte ich bereits berichtet, dass ich mit dem Expertenkreis für IT-Führungskräfte seit 2005 eine sehr lohnende, wenn auch recht aufwändige Fortbildungsmaßnahme durch meinen Technikbereich anbiete. Im Berichtszeitraum wurde die im Lauf der Jahre etablierte Netzwerk-Fortbildungsreihe fortgesetzt. Inhaltlich ist Ziel und Zweck, eine aktive Kommunikationsplattform und ein Erfahrungsnetzwerk für Fragen des technisch-organisatorischen Datenschutzes bei den aktuellen und künftigen technischen IT-Innovationen zu betreiben. Zielgruppe sind die Experten im Leitungsbereich von Rechenzentren und IT-Servicecenters sowie die behördlichen Datenschutzbeauftragten und Informations- /IT-Sicherheitsverantwortlichen (CISO) in Hochschulen und Fachhochschulen, Kommunen, Landesbehörden und anderen öffentlichen Stellen, die sich als Verantwortliche in den öffentlichen Stellen auch immer wieder neuen und komplexen datenschutzrechtlichen Herausforderungen ausgesetzt sehen. Es gilt, in einem Dauerprozess diese innovativen Entwicklungen intensiv zu analysieren, sie in ihren Gefahren- und Risikopotentialen für die informationelle Selbstbestimmung und die Datensicherheit zu bewerten und die angemessenen Schutzmaßnahmen zu entwickeln und zu implementieren. In dieser Expertenrunde sollen in Form eines Workshops der offene Gedankenaustausch zu abstrakten und individuell konkreten Bewertungen des Schutzbedarfes und der Risiken geführt sowie Lösungsansätze und mögliche gemeinsame Strategien erörtert werden. Durch Einbeziehung externer Fachleute soll zusätzlicher Wissenstransfer erzielt werden. In den letzten Jahren umfasste das Programm der Expertenkreise insbesondere folgende Schwerpunktthemen:

- Cloud Computing,
- Service Oriented Architecture (SOA) und Webtechnologie,
- Konsolidierungsstrategie,
- Virtualisierungsarchitektur,
- Umstrukturierung zu IT-Fabriken,
- Managed Storage,
- Rechner- und Dienstleistungs-Outsourcing,
- ITIL-Prozesse,
- Informationssicherheitsmanagement,
- Fernwartung,
- kabellose und berührungslose Datenübertragung/RFID/NFC,
- Kryptografie,
- biometrische Verfahren,
- datenschutzgerechtes Identitätsmanagement,
- Konversion von Netzen/Informations- und Kommunikationstechnik,
- VoIP,
- materiellrechtliche und technisch-organisatorische Fragen im TK- und Telemedienrecht.

Am 19. Mai 2011 wurde der **13. Expertenkreis** mit dem Titel **„Cloud Computing – endlose Skalierbarkeit zu Lasten des Datenschutzes?"** für IT-Führungskräfte im RZ-/IT-Dienstleistungsbereich der Hochschulen und Fachhochschulen sowie von Land und Kommunen durchgeführt. Für diese Veranstaltung konnten erfreulicherweise auch externe Referenten mit Vorträgen zu diesem sehr aktu-

ellen wie facettenreichen Thema gewonnen werden. Näheres zu den Inhalten dieser Veranstaltung wird im Beitrag Cloud Computing auf Seite 87 berichtet.
In Abstimmung mit den Teilnehmenden soll die Gesamtagenda des Expertenkreises für IT-Führungskräfte weiterentwickelt werden. Die Fortsetzung und die engagierte Themenentwicklung meines Technikreferates, die Teilnahme und Mitwirkung der Fachleute sowie das Podium mit Referenten unterschiedlicher Forschungseinrichtungen und IT-Firmen hat bereits zu einer fachlichen Etablierung im Datenschutzinstitut für die Fragen des technischen Datenschutzes und des Telemedienrechtes geführt und wird für weitere Planungen prägend sein. Das große Interesse des Teilnehmerkreises aus dem Bereich der IT-Strategie, der behördlichen Datenschutzbeauftragten und des Informationssicherheitsmanagements macht es erforderlich, meine Bemühungen um eine präventive Befassung mit neuen technischen Innovationen in meinem Datenschutzinstitut fortzusetzen.

Prävention statt Repression: Vorbeugen ist besser als Heilen …

Trotz des erheblichen und sehr individuellen fachlichen Vorbereitungsaufwandes wird mein LfD-Technikreferat diese Veranstaltungsreihe in einem sachgerechten zeitlichen Rhythmus fortsetzen. Leider mussten allerdings aus Gründen des Personalmangels und der Verdichtung im Tagesgeschäft Folgetagungen im Berichtszeitraum zunächst bis Ende 2012 ausgesetzt werden. Die Investition in die Fortbildungsangebote halte ich aufgrund der präventiven und multiplikativen Wirkung für besonders bedeutsam. Das trifft auch insbesondere auf die technischen Themen zu. Die quantitative Arbeitsbelastung ist aufgrund der geringen Personaldecke für den technischen Datenschutz allerdings weiterhin besonders hoch. Dabei entfällt fast die Hälfte aller Personentage (bezogen auf Nettoschulungstage) des Datenschutzinstituts auf die Angehörigen des Technikreferates.

… und braucht Ressourcen

Angesichts der wachsenden Bedeutung der schnelllebigen Entwicklung neuer Technologien sollte unter anderem auch deshalb zeitnah eine Verstärkung des Personals erreicht werden. Dies käme sowohl dem öffentlichen als auch dem nicht-öffentlichen Bereich der Datenschutzaufsicht zugute, weil das Technikreferat querschnittliche Dienstleistungen erbringt.

Weitere Informationen:

Unser aktuelles DsIN-Programm finden Sie unter
www.lfd.niedersachsen.de >Fortbildung/Service >Datenschutzinstitut

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.

Die Landesbeauftragte für den Datenschutz Niedersachsen