daten schutz

XX. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2009 – 2010

XX. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2009 – 2010

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

Verantwortlich: Joachim Wahlbrink

Layout: set-up design.print.media
Walderseestraße 7, 30163 Hannover

Druck: Landesvermessung und Geobasisinformation Niedersachsen
Podbielskistraße 331, 30659 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

Treffen sich zwei Referenten auf dem Flur:
„Ich muss heute noch ein Vorwort schreiben!“
„Hast du schon mal ein Vorwort gelesen, das du nicht selbst geschrieben hast?“
„Eh – nein.“
„Also?“

Wenn Sie bis hierhin gekommen sind, haben Sie eine andere Sicht der Dinge. Das ermutigt mich zu den nächsten Zeilen.

Die Videoüberwachung war in Niedersachsen das Schwerpunktthema der letzten Jahre. Dort haben wir im behördlichen wie im wirtschaftlichen Bereich neue Maßstäbe gesetzt und recht erfolgreich „aufgeräumt“.

Der politische Kurswert des Datenschutzes, also vor allem der Schutz der Privatsphäre, ist stark angestiegen. Die Resonanz in den Medien auch. Deshalb kennen Sie auch viele unserer weiteren Themen, z. B. Geodaten, Google Street View, Handyortung, elektronische Ausweiskarten, Stärkung der Medienkompetenz.

Das Hauptgewicht in diesem Bericht kommt wieder dem technisch-organisatorischen Datenschutz zu. Deshalb versuchen wir, in diesem Bereich einen über den reinen Berichtsauftrag hinausgehenden Einblick zu verschaffen, und zwar in einer Weise, die schon einen interessierten, nicht erst einen darauf spezialisierten Leserkreis erreichen möchte.

Blättern Sie doch einfach weiter. Sie werden sehen: Der Datenschutz und seine Darstellung hier sind „griffiger“ geworden.

Ich bin mir sicher, es lohnt sich.

Joachim Wahlbrink
Der Landesbeauftragte für den Datenschutz Niedersachsen

1 Datenschutz im öffentlichen Bereich

Europäischer Gerichtshof: Datenschutzaufsicht muss völlig unabhängig sein

Am 9. März 2010 hat die Große Kammer des Europäischen Gerichtshofs (EuGH, Az. C-518/07) in dem Vertragsverletzungsverfahren Europäische Kommission gegen Bundesrepublik Deutschland, über das ich bereits in meinem Tätigkeitsbericht 2005-2006 berichtete, durch Urteil festgestellt, dass die Bundesrepublik gegen ihre Verpflichtungen aus Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 verstößt.

Diese Richtlinie behandelt den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281, S. 31) und fordert, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich zuständigen Kontrollstellen ihre Aufgaben in „völliger Unabhängigkeit“ wahrnehmen (können).
In allen Bundesländern waren diese Kontrollstellen – bei unterschiedlicher Ausgestaltung im Einzelnen – jedoch staatlicher Aufsicht unterworfen. In Niedersachsen beispielsweise war die datenschutzrechtliche Kontrolle im nicht-öffentlichen Bereich als obere Aufsichtsbehörde organisiert, oberste Aufsichtsbehörde hingegen war das Niedersächsische Ministerium für Inneres und Sport (MI), das also die Fachaufsicht über diesen Bereich ausübte. Die Bundesregierung hatte in dem Verfahren vor dem EuGH die Meinung vertreten, dass die „völlige Unabhängigkeit“ der Aufsichtsbehörden immer schon dann gegeben sei, wenn die Aufsichtsbehörden „völlig unabhängig“ von den zu kontrollierenden Stellen seien.
Dieser Auffassung ist der EuGH jedoch nicht gefolgt und argumentiert in seinem Urteil wie folgt (Auszüge):

- „Im Gegenteil wird der Begriff „Unabhängigkeit“ durch das Adjektiv „völlig“ verstärkt, was eine Entscheidungsgewalt impliziert, die jeglicher Einflussnahme von außerhalb der Kontrollstelle, sei sie unmittelbar oder mittelbar, entzogen ist.“ (Rd.-Nr. 19)
- „Folglich müssen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein und nicht nur vor der Einflussnahme seitens der kontrollierten Einrichtungen.“ (Rd.-Nr. 25)

- „Nach alledem ist Art. 28 Abs. 1 Unterabs. 2 der Richtlinie 95/46 dahin auszulegen, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen." (Rd.-Nr. 30)
- „Es lässt sich aber nicht ausschließen, dass die Aufsichtsstellen, die Teil der allgemeinen Staatsverwaltung und damit der Regierung des jeweiligen Landes unterstellt sind, nicht zu objektivem Vorgehen in der Lage sind, wenn sie die Vorschriften über die Verarbeitung personenbezogener Daten auslegen und anwenden." (Rd.-Nr. 34)
- „Hinzu kommt, dass bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen. Zum einen könnte es, wie die Kommission ausführt, einen „vorauseilenden Gehorsam" der Kontrollstellen im Hinblick auf die Entscheidungspraxis der Aufsichtsstellen geben. Zum anderen erfordert die Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, also sie selbst, über jeden Verdacht der Parteilichkeit erhaben sind." (Rd.-Nr. 36)

Unmittelbar nachdem ich am Tag der Verkündung des Urteils das MI durch Übersendung einer Kopie über die Entscheidung des EuGH unterrichtet hatte, erklärte MI, dass es ab sofort keinerlei fachaufsichtsrechtlichen Weisungen (mehr) erteilen werde und sich auch aus dem so genannten Düsseldorfer Kreis, einem inoffiziellen Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, zurückziehen werde, obwohl Niedersachsen im Jahre 2010 turnusmäßig den Vorsitz in diesem Gremium inne hatte. Diese schnellen und konsequenten Entscheidungen des Ministeriums zeugen von einem hohen Maß rechtsstaatlicher Sensibilität.

Sitzung des Eurpäischen Gerichtshofes

Landtag beschließt Verfassungsänderung

Im April 2010 habe ich sodann dem MI einen Gesetzesvorschlag übersandt, der meiner Meinung nach geeignet war, die Forderungen des EuGH in Gänze umzusetzen. Der Entwurf sah vor, dass der Landesbeauftragte für den Datenschutz – vergleichbar mit dem Landesrechnungshof – eine von der Landesregierung unabhängige oberste Landesbehörde mit Sitz in Hannover wird. Um den Aufbau einer kostenintensiven eigenen „Verwaltung der Verwaltung" auszuschließen, soll er berechtigt sein, die Personalverwaltung und die Haushaltsbewirtschaftung durch eine andere öffentliche Stelle des Landes in seinem Auftrag wahrnehmen zu lassen. Nach vielen Gesprächen auf unterschiedlichsten Ebenen und zwischen unterschiedlichen Beteiligten hat der Niedersächsische Landtag auf der Grundlage eines Gesetzentwurfs der CDU-Landtagsfraktion, der wesentliche Elemente meines Vorschlags aufgegriffen hatte, am 30. Juni 2011 das Gesetz zur Neuregelung der Rechtsstellung der oder des Landesbeauftragten für den Datenschutz beschlossen. Dieses Gesetz enthält neben einer Änderung des Niedersächsischen Datenschutzgesetzes auch eine Änderung der Niedersächsischen Verfassung (Art. 62 und 66), wodurch meine unabhängige Stellung als Verfassungsorgan und als von der Landesregierung unabhängige oberste Landesbehörde in besonderer Weise verankert wird. Mit dieser, nach meinem Wissen in Deutschland einmaligen Vorgehensweise hat Niedersachsen das Urteil des EuGH in vorbildlicher Weise umgesetzt.

An etwaigen Strafzahlungen an die Europäische Kommission – diese hat bereits beim Bund angefragt, wie weit die Umsetzungen des EuGH-Urteils gediehen seien – braucht sich Niedersachsen deshalb nicht zu beteiligen.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Recht > Niedersächsisches Recht
und www.curia.europa.eu

Behördliche Datenschutzbeauftragte nicht ausreichend freigestellt

Die behördlichen Datenschutzbeauftragten (behDSB) in Niedersachsen unterstützen die öffentlichen Stellen bei der Sicherstellung des Datenschutzes und wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Sie sind in dieser Eigenschaft weisungsfrei (§ 8 a NDSG). Zu den wesentlichen Aufgabenbereichen der behDSB zählen

- die Beratung in datenschutzrechtlichen Belangen,
- die Bearbeitung von Eingaben von Bürgerinnen und Bürgern und von Beschäftigten der öffentlichen Stelle sowie
- die so genannte Vorabkontrolle von Verfahren zur Verarbeitung personenbezogener Daten durch die öffentliche Stelle.

Die Betroffenen müssen sich darauf verlassen können, dass die behDSB ihren Anliegen ernsthaft nachgehen und die Sach- und Rechtslage objektiv, also ohne einem Interessenkonflikt mit anderen dienstlichen Aufgaben ausgesetzt zu sein, beurteilen können. Allein die genannten Aufgabenbereiche lasten die in den überwiegenden Fällen nur geringfügig von anderen Aufgaben freigestellten behDSB nach meinen Erfahrungen voll und ganz aus. Eine Fortbildung ist ihnen im Hinblick auf das Zeitbudget oftmals nicht im notwendigen Umfang möglich. Das Netzwerk NORD-WEST, ein Zusammenschluss von behördlichen Datenschutzbeauftragten der Kommunen, hat in den letzten Jahren wiederholt darauf hingewiesen, dass eine wirksame Aufgabenwahrnehmung durch die behDSB eine ausreichende Freistellung von anderen Tätigkeiten erfordert.

Eine Fortbildung ist den behördlichen Datenschutzbeauftragten oftmals nicht im notwendigen Umfang möglich.

Nicht mal so nebenbei möglich

Aus meiner Sicht setzt eine den gesetzlichen Regelungen entsprechende zeitgerechte Datenschutzkontrolle bereits im präventiven Bereich ein und nicht erst dann, „wenn das Kind schon in den Brunnen gefallen ist“. Unabhängig von pressewirksamen Themen und konkreter Persönlichkeitsrechtsverletzungen bedarf es umfassender Beratung der Betroffenen zu aktuellen Themen sowie anlassfreier Prüfungen durch die behDSB. Dieser Aspekt wird von den verantwortlichen Stellen bei der Festlegung des Aufgabenbereichs des behDSB oftmals nicht berücksichtigt. Die Erledigung der Aufgaben eines behDSB ist aufgrund der Entwicklungen im datenschutzrechtlichen Bereich nicht „mal so nebenbei“ möglich. Hinweise zu dieser Problematik werden von den verantwortlichen Stellen zwar wohlwollend zur Kenntnis genommen, der Anteil der Freistellung der behDSB unter Verweis auf die bestehende Haushaltslage aber meistens nicht geändert.

In dem von mir Ende April 2010 veröffentlichten Eckpunktepapier zur Novellierung des NDSG habe ich zur Änderung der bestehenden Sachlage angeregt, eine gesetzliche Verpflichtung für die behDSB zur jährlichen Vorlage eines (Tätigkeits-)Berichts aufzunehmen, um den zuständigen politischen Gremien verdeutlichen zu können, welche Aufgabenbereiche den behDSB obliegen und wie zeitintensiv sich viele Projekte gestalten. Außerdem sollten unter Bezug auf die im BDSG vorgenommenen Änderungen zur Stärkung der Stellung der betrieblichen Datenschutzbeauftragten im Hinblick auf den Gleichbehandlungsgrundsatz auch im NDSG ergänzende Regelungen für die behDSB aufgenommen werden. Allein die Übernahme der gesetzlichen Regelung des § 4 f Abs. 3 BDSG, dass „die verantwortliche Stelle zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen hat“ in niedersächsisches Recht würde zu einer Verbesserung der Situation der behDSB führen.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Recht > Nieders.Recht > NDSG

Bürgerbüros in den Gemeinden: Vorsicht, Nachbar hört mit!

Im August und September 2010 fand eine Kontrolle der Bürgerbüros einiger selbständiger Gemeinden in Niedersachsen statt (zu Prüfungen von Kommunen hinsichtlich technisch-organisatorischer Maßnahmen siehe Beitrag auf Seite 105). Die Besuche dienten dazu, einen Eindruck über die datenschutzrechtliche Situation bei den kommunalen Gebietskörperschaften zu gewinnen, wobei der Schwerpunkt in der Beratung der ausgewählten Gemeinden lag. Die Untersuchung hat gezeigt, dass ein datenschutzrechtliches Problembewusstsein bei den verantwortlichen Personen zu erkennen ist.

Positiv …

Der Service in den Bürgerbüros beschränkt sich im Wesentlichen auf einfache Verwaltungstätigkeiten wie Änderungen in der Einwohnermeldedatei, Ausgabe von Meldebescheinigungen, Ausgabe von Ausweisen und Pässen sowie die Beglaubigung von Urkunden. Positiv fiel auf, dass bei allen Kommunen der Bereich des Bürgerbüros organisatorisch und technisch von der übrigen Verwaltung getrennt ist. Die in der Praxis häufig aus datenschutzrechtlicher Betrachtungsweise nachlässige Entsorgung von Altpapier wurde, überwiegend durch eigenes, auf das Datengeheimnis verpflichtetes Personal, datenschutzgerecht durchgeführt.

… und negativ

Oft waren Diskretionszonen und Warteräume zu klein oder fehlten völlig.

Zu bemängeln war in erster Linie die Größe der Bürgerbüros: Aufgrund der begrenzten räumlichen Möglichkeiten waren Monitore mitunter so platziert, dass diese von Bürgerinnen und Bürgern am Nachbarplatz unzulässigerweise eingesehen werden konnten. Oft waren Diskretionszonen und Warteräume zu klein oder fehlten völlig. In Verbindung mit fehlendem Schallschutz an den Wänden und Decken war es so für wartende Bürgerinnen und Bürger möglich, Gespräche mitzuhören. Zudem fehlte der Hinweis, dass Gespräche auf Wunsch der Bürgerinnen und Bürger auch in einem abgeschlossenen Büro geführt werden können. Ein weiterer Kritikpunkt war, dass die Mitarbeiterinnen und Mitarbeiter in den Bürgerbüros nicht für datenschutzrechtliche Belange sensibilisiert bzw. geschult sind.
In einigen Gemeinden können während der Besuchszeiten die einzelnen Sachbearbeiter direkt im Bürgerbüro angerufen werden. Das führt dazu, dass Telefonate durch den Sachbearbeiter angenommen werden, obwohl diesem bereits jemand gegenüber sitzt. Auf diese Weise werden Informationen übermittelt, die nicht für die wartende Person bestimmt sind. Auch der Anrufer erfährt nicht, dass seine personenbezogenen Daten auf diese Weise an Dritte übermittelt werden. Die genannten Mängel sind abzustellen.

Kontrollen werden fortgesetzt

Als Begründung für eine mangelnde Umsetzung von datenschutzrechtlichen Maßnahmen wurden vielfach Kostengründe angeführt. Die Erfahrungen haben gezeigt, dass sich viele Missstände ohne großen Aufwand abstellen lassen, oftmals durch kleine organisatorische Veränderungen. Aufgrund der gewonnenen Erkenntnisse und der positiven Unterstützung durch die behördlichen Datenschutzbeauftragten werde ich auch zukünftig landesweit Kontrollen vor Ort durchführen.

Geodaten: Uneingeschränkter Zugang für Behörden

Geodaten erlangen eine zunehmende Bedeutung für Wirtschaft und Verwaltung. Das Niedersächsische Geodateninfrastrukturgesetz regelt, unter welchen Voraussetzungen niedersächsische Behörden anderen Behörden und der Öffentlichkeit Geodaten zur Verfügung stellen.

Die „Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft" (INSPIRE-Richtlinie) schafft die organisatorischen, technischen und rechtlichen Grundlagen für eine einheitliche europäische Geodateninfrastruktur. Die Richtlinie war von den Mitgliedstaaten bis Ende 2010 in innerstaatliches Recht umzusetzen. Für niedersächsische Behörden sowie natürliche und juristische Personen des Privatrechts, die unter der Aufsicht des Landes stehen und eine öffentliche Aufgabe wahrnehmen, ist dies durch das Niedersächsische Geodateninfrastrukturgesetz (NGDIG) geschehen, das am 18. Dezember 2010 in Kraft trat. Die INSPIRE-Richtlinie und die nationalen Ausführungsgesetze richten sich also nicht unmittelbar an Wirtschaftsunternehmen wie Google mit seinem auf der Nutzung von Geodaten beruhendem Angebot Street View. Mittelbare Folgen bestehen insofern, als die geodatenhaltenden Stellen prüfen müssen, ob sie solchen Wirtschaftsunternehmen Geodaten zugänglich machen. Die Nutzung von Geodaten durch Unternehmen muss im Bundesdatenschutzgesetz geregelt werden.

Geodaten sind Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet (§ 3 Abs. 1 NGDIG). Sie beschreiben z. B. Gebiete zur Rohstoffgewinnung oder Naturschutzgebiete. Die Versicherungswirtschaft nutzt Geodaten, um Überschwemmungsgebiete auszuweisen, die zu entsprechend höheren Tarifen bei der Gebäudeversicherung führen. Geodaten sind aber auch Grundlage jedes Navigationsgeräts in einem Pkw.

Diese wenigen Beispiele zeigen das hohe wirtschaftliche Potential von Geodaten. Die Nutzung dieses Potentials europaweit zu fördern, ist Ziel der INSPIRE-Richtlinie. Daher ist es konsequent, dass das NGDIG in Übereinstimmung mit der Richtlinie den Grundsatz festlegt, dass Geodaten öffentlich zugänglich sind (§ 9 NGDIG). Die niedersächsischen Behörden und die ihnen gleichgestellten nicht-öffentlichen Stellen müssen also nicht nur anderen Behörden, sondern auch der Öffentlichkeit Geodaten zur Verfügung stellen. Nur in den insbesondere in § 10 NGDIG genannten Ausnahmefällen darf der Zugang eingeschränkt werden.

Zu kritisieren bleibt, dass der Zugang von Behörden, anders als im allgemeinen Datenschutzrecht, prinzipiell unbeschränkt gewährt wird

Aus Datenschutzsicht ist von besonderem Interesse § 10 Abs. 4 NGDIG. Danach ist der Zugang der Öffentlichkeit zu beschränken, soweit personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Diese Einschränkung gilt nicht, wenn die Betroffenen zugestimmt haben oder das öffentliche Interesse an dem Zugang überwiegt. Für den Zugang der Öffentlichkeit zu Geodaten ist also eine datenschutzgerechte Lösung gefunden worden. Zu kritisieren bleibt, dass der Zugang von Behörden, anders als im allgemeinen Datenschutzrecht, prinzipiell unbeschränkt gewährt wird.

Ich bin frühzeitig von dem Niedersächsischen Ministerium für Inneres und Sport in das Gesetzgebungsverfahren einbezogen worden, so dass bereits im Vorfeld die Klärung vieler Fragen möglich war, wenn auch nicht in allen Punkten eine Einigung erzielt werden konnte. Die nächsten Jahre werden zeigen, ob die INSPIRE-Richtlinie und die nationalen Ausführungsgesetze zu einer praxis- und datenschutzgerechten Nutzung von Geodaten führen.

ELENA-Verfahren: Beinahe noch eine Vorratsdatenspeicherung

Das ELENA-Verfahren (Elektronisches Entgeltnachweisverfahren) sorgte seit einigen Jahren für viel Gesprächsstoff. Schon in den vorangegangenen Tätigkeitsberichten habe ich darüber informiert. Im Juli 2011 wurde ELENA überraschend von der Bundesregierung eingestellt.

Das Verfahren verfolgte nach Darstellung 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. Seit Januar 2010 mussten Arbeitgeber monatlich die Datensätze der Mitarbeiter an diese Stelle übermitteln. Grundpfeiler der Innovation war die Anwendung der qualifizierten elektronischen Signatur. Hohe Einsparpotentiale bei den Unternehmen sollten ein weiterer positiver Effekt sein.

ELENA bedeutete eine Vorratsdatenspeicherung, eine millionenfache Sammlung von Daten, die in vielen Fällen nie benötigt worden wären.

Die Ausmaße des Projekts waren gewaltig: Erfasst wurden die Daten von 35 bis 40 Millionen abhängig Beschäftigten. Nicht zuletzt deshalb stieß das ELENA-Verfahren auf sehr viel Gegenwehr. Kritisiert wurde, auch von Datenschützern, die millionenfache Sammlung von Arbeitnehmerdaten (Vorratsdatenspeicherung), die in vielen Fällen nie benötigt worden wären. Ebenfalls wurde kritisiert, dass jeder Streikende in der Datenbank erfasst werden sollte. Auch der Aspekt der „Aussperrung“ sollte gemeldet werden. Hier wurden zwischenzeitlich Korrekturen vorgenommen. Kritiker sahen in dem Verfahren dennoch das Recht auf informationelle Selbstbestimmung als nicht gewahrt. Mit ELENA wäre ein digitales Abbild der Beschäftigungsverhältnisse in Deutschland entstanden. Trotz höchster Sicherheitsvorkehrungen, die auch eine Datenverschlüsselung beinhalteten, die nur im Zusammenwirken mit dem Antragsteller aufgehoben werden konnte, war nicht völlig auszuschließen, dass sich doch eines Tages Missbrauchsmöglichkeiten eröffnen könnten.

Ein Eilantrag auf Erlass einer einstweiligen Anordnung auf Aussetzung des Verfahrens wurde am 14. September 2010 durch das Bundesverfassungsgericht abgelehnt (Aktenzeichen: 1 BvR 872/10). In der Begründung wurde eingeräumt, dass die Datenspeicherung einen Grundrechtseingriff darstelle, der „ein Risiko unbefugter und missbräuchlicher Datenzugriffe schafft“. Die Richter meinten aber auch, dass es ausreicht, wenn die Verfassungsmäßigkeit der angegriffenen Bestimmungen im Hauptsacheverfahren geprüft wird. Dieses sollte 2011 folgen. Gegen das ELENA-Verfahren sind mehrere Klagen in Karlsruhe anhängig.

Neueste Entwicklungen

Die Koalitionsparteien beabsichtigten, den Beginn des zwingenden elektronischen Abrufverfahrens um zwei Jahre aufzuschieben. Folge wäre gewesen, dass es für die Jahre 2012 und 2013 den abrufberechtigten Behörden überlassen bleibt, wann diese den automatisierten Abruf aufnehmen. Hintergrund für diese Verschiebung war der Wunsch, Wege zu finden, das Abrufverfahren für die abrufenden Behörden kostengünstiger zu gestalten.
Mit Datum vom 19. Juli 2011 verständigten sich das Wirtschafts- und Arbeitsministerium überraschend darauf, „das Verfahren schnellstmöglich einzustellen“. Der notwendige datenschutzrechtliche Sicherheitsstandard sei „in absehbarer Zeit nicht flächendeckend“ zu erreichen. Inzwischen wurde das ELENA-Gesetz aufgehoben und damit die alte Rechtslage wiederhergestellt.
Gleichzeitig beschloss die Bundesregierung Eckpunkte des Bundesarbeitsministeriums für ein „projektorientiertes Meldeverfahren in der Sozialversicherung“. Dabei soll untersucht werden, wie das mit ELENA aufgebaute Wissen über neue Wege zum Datenaustausch zwischen Arbeitgebern und Sozialversicherungsträgern weiter genutzt werden kann.

Eine Zeitspanne für dieses Vorhaben gibt es noch nicht, das Thema bleibt also spannend.

Medienkompetenz:
Schüler für Datenschutz sensibilisieren!

Zur Entwicklung und Stärkung der Medienkompetenz insbesondere von Schülerinnen und Schülern haben das Land Niedersachsen und die Niedersächsische Landesmedienanstalt (NLM) das Portal „Medienkompetenz-Niedersachsen.de“ erstellt, das die vorhandenen Internetplattformen zur Medienbildung und Medienerziehung vernetzt. Darin spielt der Datenschutz leider nur eine untergeordnete Rolle. Auch aus diesem Grund geben die Datenschutzbeauftragten des Bundes und der Länder Materialien, Broschüren und Orientierungshilfen heraus und führen Informationsveranstaltungen durch, um das Bewusstsein für das Recht auf informationelle Selbstbestimmung als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker zu fördern.

So hat 2010 zum Beispiel die Initiative „Klicksafe.de“ in Zusammenarbeit mit einigen Datenschutzbeauftragten ein Zusatzmodul zu dem Lehrerhandbuch „Knowhow für junge User“ erstellt, das unter dem Titel „Ich bin öffentlich ganz privat – Datenschutz und Persönlichkeitsrechte im Web“ auf ihrer Internetseite heruntergeladen werden kann. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat eine Broschüre mit dem Titel „Meine Daten kriegt ihr nicht!“ herausgegeben.

Ergänzende Informationen sind auf der Linkliste der Arbeitsgruppe „Schule/Bildung“ der Datenschutzbeauftragten des Bundes und der Länder zu dem Themenschwerpunkt „Medienkompetenz und Datenschutz“ zu finden. Daneben gibt es auch private Organisationen, die sich mit dem Thema Medienkompetenz befassen, wie zum Beispiel in Hannover „Smiley – Verein zur Förderung der Medienkompetenz in der Arbeit mit Kindern und Jugendlichen e. V.“ (www.smiley-ev.de).

Weitere Informationen:

„Meine Daten kriegt ihr nicht“: www.hamburg.de/datenschutz
Linkliste: http://www.datenschutz.rlp.de/de/linkliste_ag_schule.php

zensus 2011
Wissen, was morgen zählt

Zensus 2011:
Datenschutzanregungen weitgehend umgesetzt

Der Zensus 2011 wird zum Stichtag 9. Mai durchgeführt. Seit diesem Zeitpunkt läuft also die Datenerhebung, deren Vorbereitung jedoch bereits mehrere Jahre in Anspruch genommen hatte.

Im Jahre 2011 wird europaweit ein Zensus, also eine Volkszählung, durchgeführt. Grundlage ist die „Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rats vom 9. Juli 2008 über Volks- und Wohnungszählungen". Auf dieser Grundlagen haben die Mitgliedsstaaten der Europäischen Union nationale Zensusgesetze erlassen, die Bundesrepublik Deutschland das „Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011)" vom 8. Juli 2009.

Anders als die Volkszählung 1987 wird der Zensus 2011 nicht als Vollerhebung durchgeführt. Es werden also nicht alle volljährigen Bürger befragt. Grundlage ist vielmehr eine Auswertung von Verwaltungsregistern. Dies sind die Melderegister, die Daten der Bundesagentur für Arbeit, Personaldaten der öffentlichen Arbeitgeber und Daten der Vermessungsverwaltung. Ergänzt wird die Registerauswertung durch eine Gebäude- und Wohnungszählung mit der Befragung aller Eigentümer von Häusern und Wohnungen. Weiterhin werden nach einem Zufallsverfahren knapp zehn Prozent der Bevölkerung für eine Haushaltsbefragung ausgewählt. Zudem erfolgt eine Befragung in so genannten Sonderbereichen, also in Wohnheimen und Gemeinschaftsunterkünften.

Die Datenschutzbeauftragten des Bundes und der Länder haben die Arbeiten an dem Zensusgesetz 2011 kritisch begleitet. Einwände haben sie z. B. gegen die Befragung in sensiblen Sonderbereichen wie Justizvollzugsanstalten und Erziehungsheimen geäußert. In diesen Einrichtungen werden nun nicht die Bewohner, sondern nur die Einrichtungsleitungen befragt. Grundsätzliche Bedenken gegen die Verfassungsmäßigkeit des Zensus 2011 wurden von den Datenschutzbeauftragten des Bundes und der Länder jedoch nicht vorgebracht. Insbesondere legt das Zensusgesetz 2011, einer zentralen Forderung des Bundesverfassungsgerichts in dem so genannten Volkszählungsurteil vom 15.12.1983 folgend, zur Wahrung des Statistikgeheimnisses die Abschottung der Erhebungsstellen von den anderen Stellen der Verwaltung eindeutig fest.

Mit Beschluss vom 21. September 2010 (Az.: 1 BvR 1865/10) hat das Bundesverfassungsgericht eine gegen das Zensusgesetz 2011 gerichtete Verfassungsbeschwerde wegen ihrer mangelnden Bestimmtheit nicht zur Entscheidung angenommen. Es bleibt abzuwarten, ob andere, nach Auffassung des Bundes-

Quelle:
www.zensus2011.de

verfassungsgerichts substantiiertere Verfassungsbeschwerden, zu einer anderen Entscheidung führen werden.

Unabhängig von grundsätzlichen verfassungsrechtlichen Überlegungen kommt es nun darauf an, das Zensusgesetz 2011 datenschutzgerecht umzusetzen. Zu diesem Zweck wurde in Niedersachsen das „Niedersächsische Ausführungsgesetz zum Zensusgesetz 2011" vom 6. Oktober 2010 verabschiedet. Das Gesetz regelt insbesondere die Einrichtung der örtlichen Erhebungsstellen (Gemeinden mit mindestens 30.000 Einwohnern und die Landkreise) und den Einsatz von Erhebungsbeauftragten. Breiten Raum nimmt die Gewährleistung einer Abschottung der Erhebungsstellen ein. Konkretisiert wird das Ausführungsgesetz durch detaillierte Verwaltungsvorschriften. Weiterhin sind den örtlichen Erhebungsstellen eine Musterdienstanweisung für die Durchführung des Zensus sowie Informationen und Empfehlungen („Module") zur IT-Ausstattung, zur Einrichtung der Erhebungsstellen und zur Werbung von Erhebungsbeauftragten zur Verfügung gestellt worden.

Sowohl das Ausführungsgesetz und die Verwaltungsvorschriften als auch die ausführlichen und für die örtlichen Erhebungsstellen hilfreichen Module hat das Niedersächsische Ministerium für Inneres und Sport mit mir frühzeitig abgestimmt. Meine Anregungen wurden weitgehend umgesetzt.

Erste Ergebnisse, nämlich die Bekanntgabe der Einwohnerzahl, sind ab November 2012 zu erwarten.

Antworten auf häufig gestellte Fragen (FAQ):
Homepage des Bundesbeauftragten für den Datenschutz und die Informationssicherheit
www.bfdi.bund.de.

Der neue elektronische Personalausweis: Zusatzfunktionen verlangen erhöhte Aufmerksamkeit

Seit dem 1. November 2010 erhalten Bürgerinnen und Bürger auf Antrag den neuen elektronischen Personalausweis (nPA) nach dem novellierten „Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften" vom 18.Juni 2009.

Der neue Personalausweis hat nunmehr Scheckkartenformat und enthält sichtbar aufgedruckt in etwa die gleichen personenbezogenen Daten wie das alte Dokument. Neu ist der kontaktlos auslesbare RFID-Chip, der u. a. Vornamen, Nachnamen, Tag und Ort der Geburt, Anschrift und gegebenenfalls Doktorgrad und Künstlername elektronisch speichert. Ebenfalls sind dort biometrische Daten des Gesichtsbildes sowie – auf ausdrücklichen Wunsch der Ausweisinhaberin oder des Ausweisinhabers – zwei Fingerabdrücke abgelegt, die allerdings nur im Rahmen hoheitlicher Identitätskontrollen ausgelesen werden können. Die Datenschutzbeauftragten des Bundes und der Länder wurden frühzeitig in die Projektplanungen einbezogen. Vielen Anforderungen, um die bei der Einführung des elektronischen Reisepasses noch hart gerungen werden musste, wurde von Beginn an entsprochen. Dennoch ist eine komplexe Infrastruktur entstanden, die insbesondere bezüglich der Zusatzfunktionen erhöhte Aufmerksamkeit – nicht zuletzt auch des Bürgers – erfordert.

Elektronischer Identitätsnachweis (eID-Funktion)

Über die herkömmliche Ausweisfunktion hinaus kann der neue Personalausweis auch als elektronischer Identitätsnachweis im Internet genutzt werden. Die eID-Funktion ermöglicht es dem Ausweisinhaber, sich sowohl im E-Government (z. B. zur Abwicklung von Verwaltungsleistungen mit Gemeinden, bei der Kfz-Ummeldung oder zur Beantragung von Geburtsurkunden) als auch im E-Commerce (z. B. für Einkäufe in Online-Shops oder zur Nutzung von Online-Services von Banken und Versicherungen) gegenüber berechtigten Stellen zu identifizieren. Zu diesem Zweck erteilt das Bundesverwaltungsamt Behörden und Unternehmen (so genannte Diensteanbieter) auf Antrag und nach Überprüfung des angegebenen Zwecks für die Auslesung ein Berechtigungszertifikat, in dem festgelegt ist, welche Daten (z. B. Vor- und Familienname, Geburtstag und -ort, Anschrift oder Angabe, ob ein bestimmtes Alter überschritten ist,) elektronisch aus dem Ausweis ausgelesen werden dürfen.
In Zusammenarbeit zwischen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, einigen Landesdatenschutzbeauftragten und der Vergabestelle für Berechtigungszertifikate des Bundesverwaltungsamtes wurden hierfür

Leitlinien für die Vergabe von Berechtigungen für Diensteanbieter unter
www.datenschutzzentrum.de/neuer-Personalausweis/20100910-Leitlinien-npa.pdf

Quelle: Bundesministerium des Inneren

datenschutzrechtliche Leitlinien für die Vergabe von Berechtigungen für Diensteanbieter nach § 21 Abs. Personalausweisgesetz (PAuswG) erarbeitet.
Die eID-Funktion ist bei der Ausgabe des neuen elektronischen Personalausweises an über 16-jährige Personen standardmäßig aktiviert, kann aber abgeschaltet werden, wenn die Ausweisinhaberin oder der Ausweisinhaber die Funktion nicht nutzen möchte. Die Nutzung der eID-Funktion ist somit freiwillig. Um den elektronischen Identitätsnachweis über das Internet nutzen zu können, werden eine spezielle Software benötigt, die so genannte Ausweis-Applikation (kurz: AusweisApp), ein zertifiziertes Kartenlesegerät, das an den eigenen Personalcomputer angeschlossen wird und Daten des Personalausweises per kontaktloser Schnittstelle auslesen kann, sowie eine sechsstellige PIN. Im Anwendungsfall wird dem Ausweisinhaber zunächst das Berechtigungszertifikat des Diensteanbieters mit allen wichtigen Informationen zum jeweiligen Online-Dienst angezeigt und genau aufgelistet, welche Ausweisdaten übermittelt werden sollen. Dabei besteht die Gelegenheit, das Auslesen einzelner Datenfelder zu unterbinden, was möglicherweise allerdings auch bewirkt, dass ein Online-Dienst nicht mehr erbracht werden kann. Die durch den Ausweisinhaber freigegebenen Daten werden dann ausgelesen und in verschlüsselter Form an den Diensteanbieter übermittelt, wenn der Ausweisinhaber seine PIN eingegeben hat.

Von Lesegeräten ohne Tastatur wird abgeraten

Um Missbrauchsmöglichkeiten zu verhindern, besteht eine jederzeitige Möglichkeit, abhanden gekommene Ausweise mit einem Sperrkennwort durch Eintragung in eine Sperrliste als ungültig erklären zu lassen. Daneben kann die PIN auch jederzeit von zu Hause oder in der Personalausweisbehörde geändert werden. Der Bund möchte Anreize für den Einsatz der eID-Funktion schaffen und beabsichtigt, in der Anfangsphase Kartenlesegeräte im Wert von bis zu 24 Millionen Euro zu „sponsern". Entgegen der Empfehlung der Datenschutzbeauftragten ist diese Förderung bisher leider nur für so genannte Basislesegeräte ohne eigene Tastatur vorgesehen. Erfolgt die Eingabe der sechsstelligen PIN jedoch über die Tastatur des PC, besteht die Gefahr, dass Kriminelle über eingeschleuste Schad-

software (z. B. Trojaner, korrekt: trojanische Pferde) die PIN mitlesen und in der Folge unbemerkt die eID-Funktion des Ausweises für eigene Zwecke missbräuchlich nutzen können.

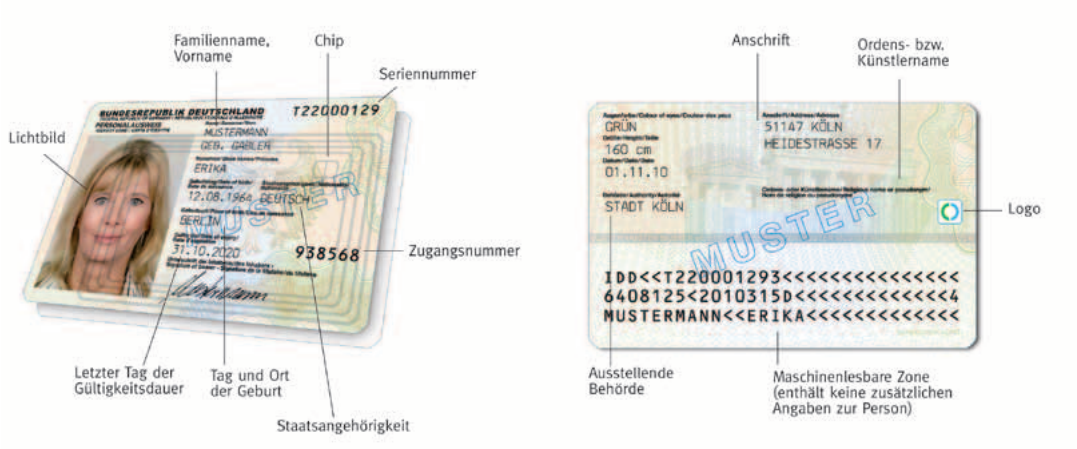
So sind für den verantwortungsvollen Einsatz der eID-Funktion aus datenschutzrechtlicher Sicht vor allem folgende Punkte zu beachten:

- Es sollten möglichst nur Standard- oder Komfortlesegeräte zum Einsatz kommen, die mit eigenem Tastaturfeld ein missbräuchliches Auslesen der PIN verhindern. Diese sind darüber hinaus auch in vielen anderen Anwendungsbereichen einsetzbar, Komfortlesegeräte z. B. im Rahmen der Nutzung der „Qualifizierten elektronischen Signatur".
- Steht nur ein Basislesegerät zur Verfügung, sollte für die Eingabe der PIN zumindest die Bildschirmtastatur der AusweisApp genutzt werden.
- Unverzichtbar ist der Schutz des jeweilig genutzten PCs mit der aktuellsten Antivirensoftware und einer Firewall.
- Weiterhin wichtig sind regelmäßige Sicherheitsupdates für Betriebssystem, Browser und Anwendungssoftware.

Qualifizierte elektronische Signatur nicht mit Basislesegerät

Zusätzlich kann auf dem neuen elektronischen Personalausweis eine Signaturfunktion eingerichtet werden, mit deren Hilfe eine elektronische Unterschrift z.B. für rechtwirksame Verträge oder Anträge im Internet geleistet werden kann, soweit diese der Schriftform bedürfen. Im Unterschied zur eID-Funktion wird die Signaturfunktion nur auf Antrag aufgebracht. Sie ist also ebenfalls freiwillig.

Möchte ein Ausweisinhaber künftig mit Hilfe des neuen elektronischen Personalausweises elektronisch unterschreiben können, muss er selbst die Aktivierung der Signaturfunktion bei einem sogenannten Zertifizierungsdiensteanbieter beantragen. Erst dann wird ein Signaturschlüsselpaar erzeugt und das entsprechende Zertifikat in den Ausweis übertragen.



Quelle: Bundesministerium des Inneren

Die Datenschutzbeauftragten haben in der Vergangenheit immer wieder vergeblich für eine Anschubfinanzierung in Form kostenloser oder subventionierter Signaturschlüssel plädiert.

Qualifizierte Signaturen können sodann mittels Eingabe einer zweiten PIN, die sich von der sechsstelligen PIN der eID-Funktion unterscheiden muss, erzeugt werden. Hierbei ist zu beachten, dass Kartenlesegeräte ohne eigenes Tastaturfeld zur Erzeugung einer qualifizierten Signatur ungeeignet sind und die Bürgerinnen und Bürger zudem die Kosten, die der Zertifizierungsdiensteanbieter für Zertifkatserteilung und Signatur erhebt, bisher noch allein zu tragen haben. Es ist daher zu erwarten, dass dieses zunächst die Verbreitung der Nutzung der Signaturfunktion hemmen wird. Zur Förderung dieser Sicherheitstechnologie haben die Datenschutzbeauftragten des Bundes und der Länder in der Vergangenheit immer wieder für eine Anschubfinanzierung in Form kostenloser oder subventionierter Signaturschlüssel plädiert – leider vergeblich.

Neben den Bürgern werden auch die Personalausweisbehörden durch die Einführung des elektronischen Personalausweises mit ungewohnten Abläufen und Funktionen konfrontiert und erhalten völlig neue Aufgaben bei der Erstellung, Ausgabe, Änderung oder Sperrung des elektronischen Personalausweises. Der elektronische Personalausweis wird aufgrund seiner Zusatzfunktionen für Zwecke der elektronischen Abwicklung von Rechtsgeschäften und des E-Government einerseits vielfältige Chancen bieten, zum anderen aber auch einige neue Gefahren hinsichtlich des Datenschutzes und der Datensicherheit mit sich bringen.

Ich werde auch in Zukunft die Anwendungsfelder des neuen elektronischen Personalausweises, die Weiterentwicklung der technologischen Entwicklung im Bereich der Hardware und der Ausweis-Applikationen sowie die organisatorischen Abläufe beobachten. Der Prüfungsalltag in allen Bundesländern und in den kommunalen Behörden wird ergeben, inwieweit Nachbesserungen im Sinne der informationellen Selbstbestimmung für diese neue Infrastruktur erforderlich werden.

Weitere Informationen: www.personalausweisportal.de

NEPS, PISA, TIMSS, IGLU: Datenbedarf für Bildungsforschung nimmt zu

An Schulen werden heutzutage immer wieder Erhebungen im Rahmen von nationalen oder internationalen Schulleistungsstudien durchgeführt, um Rückschlüsse auf den Stand bestimmter Fähigkeiten von Schülerinnen und Schülern und die Einflüsse auf diese je nach Alter, Herkunft oder sozialem Umfeld ziehen zu können. Aufgrund dieser Erkenntnisse können dann z. B. Entwicklungsplanungen im Bereich von Schule, Hochschule oder Ausbildung besser gelenkt sowie die Entwicklung von Bildungsplänen begleitet werden. Da im Rahmen dieser Studien umfangreiche personenbezogene Daten durch verschiedene beteiligte Personen und Stellen verarbeitet werden, spielt die Beachtung des Datenschutzes eine wichtige Rolle.

Da der lebenslange Erwerb von Wissen und Fähigkeiten weltweit zu den Schlüsselfaktoren für ein beruflich und gesellschaftlich erfolgreiches Leben geworden ist, ist es daher von entscheidender Bedeutung zu verstehen, wie sich Bildungswege entfalten und wie sich Kompetenzen in der Wechselwirkung zwischen Bildungseinrichtungen, Familie und Arbeitsplatz lebenslang entwickeln. Die hierfür notwendigen Daten liegen bisher nicht vor. Deswegen hat das Bundesministerium für Bildung und Forschung 2008 das Nationale Bildungspanel (National Educational Panel Study – NEPS) ins Leben gerufen. NEPS ist die bisher größte nationale Langzeitstudie im Bereich der Bildungsforschung. Im Mittelpunkt steht die Untersuchung von Bildungsprozessen, Bildungsentscheidungen und Bildungserträgen über die gesamte Lebensspanne. Um hierfür repräsentative Daten zu erlangen, wird im Rahmen von NEPS die Entwicklung von Kompetenzen im Kleinkindalter, im Kindergarten, im allgemeinbildenden Schulsystem, in der beruflichen Ausbildung, im Studium und im Arbeitsleben untersucht.
Dafür werden in den kommenden Jahren jährlich rund 60.000 Personen in ganz Deutschland befragt und getestet; die Altersspanne der Personen, über die Daten erhoben werden, liegt zwischen 0 und 64 Jahren. Im allgemeinen Schulsystem sollen ab 2010 etwa 1.000 Schulen und 30.000 Schüler an den Erhebungen teilnehmen.

Telefoninterviews sind generell freiwillig

Im Herbst 2010 erfolgte die erste Runde der NEPS-Haupterhebung in den Jahrgangsstufen 5 und 9 in insgesamt 655 Schulen. Pro Schule wurden ein bis zwei Klassen eines Jahrgangs in einem Zufallsverfahren für die Teilnahme ausgewählt. Dabei wurden die Schüler, die Schulleitung und die in den ausgewählten Klassen unterrichtenden Klassen-, Mathematik- und Deutschlehrer schriftlich sowie die Eltern im Rahmen eines Telefoninterviews befragt. Die Teilnahme war generell freiwillig.

Im Rahmen des Genehmigungsverfahrens der NEPS-Haupterhebung hat das Niedersächsische Kultusministerium mich im Sommer 2010 im Vorfeld beteiligt, da in diesem Zusammenhang eine Vielzahl von personenbezogenen Daten erhoben wird. Es waren daher von mir die so genannte Prozedurbeschreibung sowie die Unterlagen zur Durchführung der Studie wie Erfassungsbögen und Informationsbriefe auf Datenschutzkonformität zu überprüfen. Die an der Studie beteiligten Institute IEA DPC und infas speichern die Namen und Kontaktdaten der teilnehmenden Schüler und Eltern ausschließlich zur späteren Kontaktaufnahme für Folgeerhebungen. Diese Speicherung erfolgt getrennt von den übrigen Erhebungsdaten.

Erfreuliches Datenschutzniveau

Die Struktur der NEPS-Haupterhebung lehnt sich an die Erhebungsprozeduren anderer bereits genehmigter und durchgeführter und somit auch aus datenschutzrechtlicher Sicht überprüfter Schulleistungsstudien wie z. B. PISA, TIMSS oder IGLU an. Daher waren sowohl die Prozedurbeschreibung als auch die Erfassungs- und Fragebögen sowie die Informationsschreiben und Einwilligungserklärungen im Großen und Ganzen bereits datenschutzkonform ausgestaltet, so dass ich bei der Überprüfung nur wenige Hinweise zum Datenschutz geben musste, zum Beispiel hinsichtlich der Vernichtung der Erhebungsunterlagen in den Schulen, der Benennung eines Ansprechpartners im Schüleranschreiben und der Bitte um einen deutlicheren Hinweis auf die Freiwilligkeit der Angaben durch die Eltern im Telefoninterview. Eine Ende 2010 erfolgte weitere Überprüfung einer für das Frühjahr 2011 geplanten NEPS-Folgeerhebung im 9. Jahrgang an Schulen der Sekundarstufe I und an Förderschulen konnte daraufhin erfreulicherweise ohne datenschutzrechtliche Anmerkungen meinerseits abgeschlossen werden. Zur Zeit prüfe ich drei weitere begleitende Studien zu NEPS: NEPS-Folgeerhebung 2011 im 6. Jahrgang, NEPS-Entwicklungsstudie 2011 im 9. Jahrgang und NEPS-Vergleichsstudie 2011 im 5. und 6. Jahrgang.
Da ich seit dem Jahreswechsel 2010/2011 neben den fünf NEPS-Studien bereits zu acht weiteren Schulleistungsstudien (Bildungsstandards – Normierungsstudie Naturwissenschaften, IGLU/TIMSS Haupterhebung, Bildungsstandards Ländervergleich Primarstufe, Validierungsstudie, SINUS-Videostudie, SINUS an Grundschulen, ADDITION sowie Pilotierungsstudie – Billdungsstandards) um Beteiligung in den Genehmigungsverfahren gebeten worden bin, zeichnet sich bereits ab, dass künftig sowohl mit einer zunehmenden Anzahl als auch mit einer regelmäßigen Wiederholung derartiger Studien in bestimmten Rhythmen zu rechnen ist und dadurch vermehrt entsprechende Aufgaben auf mich zukommen werden.

Weitere Informationen:

NEPS: www.neps-studie.de
TIMSS: www.ifs-dortmund.de/1269.html www.bmbf.de/de/6628.php
IGLU: www.ifs-dortmund.de/pirls2011.html www.bmbf.de/de/6626,php
Normierungsstudie Naturwissenschaften:
www.iqb.hu-berlin.de/ arbbereiche/projekte/?2pg=p_34

2

Datenschutz in der Wirtschaft

Dem gläsernen Menschen entgegenwirken – deutliche Verstärkung des Datenschutzes im nicht-öffentlichen Bereich

Der Begriff „Gläserner Mensch“ als bildhaftes Gleichnis aus dem Bereich des Datenschutzes wird bereits seit längerem für eine als kritisch zu bewertende umfassende Durchleuchtung des Menschen und seines Verhaltens durch einen auf Überwachung angelegten Staat verwendet. Instrumente wie etwa die staatliche Kontenabfrage, die Vorratsdatenspeicherung oder Onlineüberwachung sowie die immer weiter um sich greifende Videoüberwachung im staatlichen Bereich bilden nur einige Beispiele hierfür. Einher geht hiermit seit längerer Zeit ein zunehmender Verlust an Privatsphäre und des Rechts auf informationelle Selbstbestimmung.

Nicht erst seit gestern ist der Begriff vom „Gläsernen Menschen“ aber auch immer öfter auf die Durchleuchtung und Erfassung des Menschen durch Einrichtungen und Unternehmen außerhalb des Staates zutreffend. So kennen wir heute klare Tendenzen zum „Gläsernen Patienten“, zum „Gläsernen Mitarbeiter“ oder „Gläsernen Kunden“. Für den „Gläsernen Menschen“ stehen hier aus Datenschutzsicht Instrumente und Geschäftsfelder wie die ausufernde Videoüberwachung in Geschäften, Restaurants oder Einkaufsgalerien oder etwa die Tätigkeit von Adresshändlern und Auskunfteien. Zahlreiche Firmen unternehmen erhebliche Anstrengungen, persönliche Vorlieben oder das Kauf- oder Zahlungsverhalten zu erforschen und Kundenprofile insbesondere zu Werbezwecken zu erstellen.
Das Internet spielt nicht nur in diesem Zusammenhang eine sich immer dynamischer entwickelnde Rolle im Hinblick auf Anmelde-, Bestell- oder Buchungsvorgänge, sondern auch bei der Fülle der zahlreichen sozialen Netzwerke wie Facebook, My Space oder StudiVZ. Diese entfalten ihre besondere Anziehungskraft durch ihren unentgeltlichen Zugang, wobei sie sich in der Regel über Werbung finanzieren. Besorgniserregend ist in diesem Zusammenhang, wie viele Netzwerkmitglieder Privates öffentlich machen und damit den sogenannten Selbstdatenschutz total vernachlässigen. Insbesondere Datenschutzskandale rund um die unzulässige Überwachung von Beschäftigten in Wirtschaftsunternehmen im Sinne eines „Gläsernen Mitarbeiters“ haben deshalb seit einiger Zeit immer stärkere Rufe nach einer Verstärkung des Datenschutzes im nicht-öffentlichen Bereich ausgelöst.

Neuausrichtung der Datenschutzaufsicht

Diese Verstärkung und gleichzeitige Neuausrichtung der niedersächsischen Datenschutzaufsicht im nicht-öffentlichen Bereich ist im Frühjahr des Jahres 2009 eingeleitet worden und hat im März 2010 ihren vorläufigen Abschluss gefunden. Während die entsprechenden Aufgaben bis dahin nur mit einem Team von fünf Mitarbeitern wahrgenommen wurden, sind nunmehr unter einer eigenständigen Leitung elf Mitarbeiterinnen und Mitarbeiter in drei Teams tätig. Davon mit umfasst ist insbesondere auch eine

Stelle für den technisch-organisatorischen Datenschutz, der neben den rein rechtlichen Anforderungen im Datenschutz einen immer größeren Stellenwert erlangt.

Siehe hierzu auch den Beitrag „Europäischer Gerichtshof …" auf Seite 8.

Die Neuausrichtung des Datenschutzes im nicht-öffentlichen Bereich geht neben dieser personellen Verstärkung ausdrücklich von einem präventiven und einem „repressiven" Ansatz aus. Im präventiven Bereich ging es dabei darum, die Beratungstätigkeit zielorientiert und auch branchenspezifisch weiterzuentwickeln und die Aufmerksamkeit für den Datenschutz zu erhöhen. Aufgrund der verstärkten Personalausstattung ist es möglich, sowohl Einzelpersonen als auch Wirtschaftsunternehmen im weitaus stärkerem Maße als bisher zu beraten. Neben Fragen des technisch-organisatorischen Datenschutzes und Problemen des Datenschutzes bei der Telemediennutzung (Internet) nehmen dabei gerade auch Fragen von Bürgerinnen und Bürgern zu ihren Rechten auf Auskunft, Löschung und Sperrung von Daten sowie zu den Erfordernissen einer datenschutzkonformen Einwilligung in Datenverarbeitungen einen breiten Raum ein.

Vernetzung mit den betrieblichen Datenschutzbeauftragten

Eine besondere Bedeutung für den Bereich der Wirtschaft kam hierbei einer verstärkten Vernetzung mit den betrieblichen Datenschutzbeauftragten zu. Bereits bislang habe ich teilgenommen an den jeweils zwei- bis dreimal im Jahr stattfindenden Erfahrungs- und Austauschkreisen von insgesamt 60 betrieblichen Datenschutzbeauftragten aus vielfältigen Branchen wie Industrie, IT-Dienste, Gesundheitsdienstleister, Finanzen, Banken, Versicherungen, produzierendem Gewerbe, Touristik, Handel, Rechtsanwälten sowie selbständigen externen Datenschutzbeauftragten. Hierbei sind auch namhafte Unternehmen der niedersächsischen Wirtschaft vertreten. Aufgrund meiner nunmehr personell verstärkten und damit intensivierten Teilnahme an diesen Besprechungen können in deutlich stärkerem und differenzierterem Maße Themen der Datenschutzaufsicht eingebracht werden. Gerade im Vorfeld künftiger Datenverarbeitungsverfahren können hierbei vertrauensbildende Maßnahmen greifen und eine wirksame Beratungstätigkeit entfaltet werden. Zudem erhalte ich bei dieser Gelegenheit vermehrt Informationen und Erkenntnisse aus der Praxis der Unternehmen und kann diese in der eigenen Aufsichtstätigkeit verwenden.

Um darüber hinaus möglichst viele Einzelbetriebe der Wirtschaft und des Handwerks zu erreichen, wurden Kontakte zu den niedersächsischen Industrie- und Handelskammern und zu Vertretern der entsprechenden Handwerkskammern gesucht. Hierbei wurde eine fachliche Unterstützung bei den dort wahrgenommenen Beratungstätigkeiten zugesagt; gleichzeitig wurden bereits in diversen Kammerzeitungen datenschutzrechtliche Themen aufgegriffen.

Außer dieser gezielten Beratung von Unternehmen galt es auch, dem stark gestiegenen Informationsbedürfnis der Bürgerinnen und Bürger Rechnung zu tragen. Gleichzeitig ist hier der Erkenntnis zu folgen, dass Datenschutz neben seiner behördlich-repressiven Komponente vornehmlich eine Bildungs- und Erziehungsaufgabe ist. Diese muss insbesondere eine Sensibilisierung für den Umgang mit personenbezogenen Daten zum Gegenstand haben. Neben der intensivierten Informationsweitergabe über das von mir betriebene Datenschutzinstitut Niedersachsen (DsIN; siehe Beitrag auf Seite122), die Medien, das Internet sowie über Broschüren etc. ist daher auch die Zusammenarbeit mit externen Einrichtungen geprüft worden. Hierbei ist es unter anderem zur Kontaktaufnahme mit der Verbraucherzentrale Niedersachsen (VZN) gekommen. Grundsätzlich ist in diesem Zusammenhang festzustellen. dass die Verbraucherzentralen und ihr Bundesverband im Rahmen ihrer Beratungen zum Verbraucherrecht auch

zum Datenschutz erhebliche Anstrengungen unternehmen und die Entwicklung des Datenschutzes in Deutschland durch eigene Initiativen und Stellungnahmen sehr aktiv begleiten. Aus diesem Grunde bietet sich die VZN als besonderer Kooperationspartner für die Datenschutzaufsichtsbehörde an. Diesem folgend ist der VZN eine Unterstützung bei ihrer Beratungstätigkeit und bei der Erstellung von Informationsmaterial angeboten worden.

Datenschutzprüfungen und Sanktionen

Neben dieser präventiven Säule der Datenschutzaufsicht kommt den eher repressiven Aufgaben in Gestalt von Datenschutzprüfungen bis hin zur Verhängung von Sanktionen besondere Bedeutung zu. Angestoßen wurden solche Maßnahmen vielfach durch eine beträchtliche Anzahl von datenschutzrechtlichen Eingaben von Bürgerinnen und Bürgern oder sonstigen Petenten. Aufgrund der personellen Verstärkung des Datenschutzes im nicht-öffentlichen Bereich konnte solchen Eingaben in größerer Tiefe und zeitnäher nachgegangen werden. Deshalb sind im Berichtszeitraum auch eine Fülle von förmlichen Maßnahmen bis zur Verhängung von Bußgeldern (siehe hierzu Seite 62 dieses Tätigkeitsberichts) ergriffen, aber auch „schlichte“ Hinweise gegeben worden mit dem Ziel, datenschutzkonformes Verhalten durchzusetzen. In diesem Rahmen kann die Aufsichtsbehörde vor allem auch Vorort-Prüfungen in den Geschäftsräumen von Unternehmen und Betrieben vornehmen und ggf. im Wege des Verwaltungszwangs oder der Durchführung von Ordnungswidrigkeitenverfahren auch Maßnahmen zur Durchsetzung des Datenschutzes ergreifen. Wichtig ist in diesem Zusammenhang, dass nach einer der jüngsten Novellen des BDSG auch materiell unzulässige Datenverarbeitungen untersagt werden können. Bislang war die Untersagung einzelner Verfahren nur bei Verstößen gegen technisch-organisatorische Vorgaben möglich.
Erwähnenswert sind in diesem Zusammenhang besonders folgende durchgeführte Maßnahmen:

- schriftliches Datenschutzkontrollverfahren bei rund 50 Zeitarbeitsfirmen im Hinblick auf die Frage der Bestellung von Datenschutzbeauftragten (siehe Seite 60),
- zahlreiche Vorort-Kontrollen zum Thema Videoüberwachung im nicht-öffentlichen Bereich (§ 6 b BDSG; siehe Seite 116),
- Kontrollen bei Callcentern im Hinblick auf die von diesen regelmäßig betriebene Auftragsdatenverarbeitung nach § 11 BDSG bzw. zur Mitarbeiterüberwachung in Form von Gesprächsaufzeichnung bzw. Mithören von Gesprächen (siehe Seite 32).

Fazit

Als Ergebnis der bisherigen Entwicklung ist festzuhalten, dass die Neuausrichtung des Datenschutzes im nicht-öffentlichen Bereich und die bisher realisierte Personalverstärkung insbesondere im Bereich der Beratung, Bearbeitung von Eingaben und der Verfolgung von Datenschutzverstößen bereits zu einer deutlichen Stärkung der Tätigkeit der Behörde geführt hat. Auch die künftige Tätigkeit wird sich dementsprechend an den besonderen datenschutzrechtlichen Risiken und Auffälligkeiten in den verschiedenen Branchen des nicht-öffentlichen Bereichs orientieren. Hierbei wird auch den Erkenntnissen aus dem Erfahrungsaustausch zwischen den Datenschutzaufsichtsbehörden der Länder besondere Bedeutung zukommen.

Beschäftigtendatenschutz: Gesetzentwurf dringend verbesserungsbedürftig

Der Beschäftigten- oder auch Arbeitnehmerdatenschutz ist bereits großes Thema meines letzten Tätigkeitsberichts gewesen. Damals war die systematische Überwachung von Beschäftigten eines großen Lebensmitteldiscounters durch Detekteien und andere Sicherheitsunternehmen bekannt geworden. Dieser bundesweit diskutierte Vorgang, in dem die Datenschutzaufsichtsbehörden der Länder erhebliche Datenschutzverstöße festgestellt und Bußgelder in Höhe von insgesamt rund 1,5 Millionen. Euro verhängt hatten, war kein Einzelfall. In der Folgezeit wurden bundesweit viele weitere Datenschutzverstöße in anderen Unternehmen publik.

Die zahlreichen datenschutzrechtlichen „Skandalfälle" haben in den Blickpunkt gerückt, dass in Deutschland bislang eine einheitliche datenschutzrechtliche Regelung fehlt, die den spezifischen Besonderheiten des Arbeitsverhältnisses Rechnung trägt. Trotz seiner großen Bedeutung – und der von Seiten des Datenschutzes seit Jahrzehnten erhobenen Forderung nach einer gesetzlichen Regelung – ist der Arbeitnehmerdatenschutz dennoch bislang nur rudimentär geregelt. Arbeitnehmer und Arbeitgeber sind daher darauf angewiesen, sich in Datenschutzfragen durch eine zunehmend unübersichtlicher werdende Vielzahl von gerichtlichen Einzelfallentscheidungen zu arbeiten und sich an den zu allgemeinen Regelungen des Bundesdatenschutzgesetzes zu orientieren.

Zahlreiche Problemfelder

Zahlreiche Beispiele zu Datenschutzverstößen im Bereich des Beschäftigtendatenschutzes finden sich auch z.B. im 22. Tätigkeitsbericht 2007 und 2008 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de.

Durch klarere gesetzliche Regelungen kann die Rechtssicherheit für Beschäftigte und Arbeitgeber erhöht werden. Als Problemfelder im Bereich des Arbeitnehmerdatenschutzes haben sich insbesondere die folgenden Punkte herausgestellt:

- Erhebung und Verwendung von Daten eines Bewerbers im Einstellungsverfahren,
- Umfang der Zulässigkeit von gesundheitlichen Untersuchungen im Einstellungsverfahren,
- Datenschutz bei Einstellungstests,
- Datenerhebung und -verwendung in laufenden Beschäftigungsverhältnissen,
- Videoüberwachung am Arbeitsplatz,
- Datenerhebung bei der Nutzung von Telefon, E-Mail und Internet am Arbeitsplatz,
- Verantwortlichkeit für die Einhaltung datenschutzrechtlicher Vorschriften, wenn der Arbeitgeber Beschäftigtendaten durch Dritte erheben oder verarbeiten lässt,
- Sicherstellung einer wirksamen innerbetrieblichen Datenschutzkontrolle.

Der erste Schritt 2009: § 32 Bundesdatenschutzgesetz

Zum 1. September 2009 ist mit § 32 eine besondere Regelung in das Bundesdatenschutzgesetz (BDSG) eingefügt worden, welche die Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses zum Inhalt hat. Die neue Bestimmung lässt jedoch eine Reihe dringender Fragen des Arbeitnehmerdatenschutzes offen.

Die am 27. September 2009 gewählte Bundesregierung hat unter Verzicht auf ein eigenständiges Beschäftigtendatenschutzgesetz am 25. August 2010 den Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes eingebracht. Mit diesem Gesetz soll ein neuer Unterabschnitt mit dem Titel „Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses" in das Bundesdatenschutzgesetz eingefügt werden. Der Gesetzentwurf verfolgt ausweislich seiner Begründung das Ziel, einerseits die Beschäftigten vor der unrechtmäßigen Erhebung und Verwendung ihrer personenbezogenen Daten zu schützen und andererseits das Informationsinteresse des Arbeitgebers zu beachten. Beides diene dazu, ein vertrauensvolles Arbeitsklima zwischen Arbeitgebern und Beschäftigten am Arbeitsplatz zu unterstützen.

Aktuelle niedersächsische Beispiele aus dem Bereich des Beschäftigtendatenschutzes Niedersachsen finden sich in meiner aktuellen Sammlung „Fälle aus der Praxis" im Internet unter www.lfd.niedersachsen.de Pfad: Fortbildung > Fälle aus der Praxis

Der zweite Schritt 2011?

Zum Zeitpunkt der Drucklegung dieses Berichts befand sich der Gesetzentwurf im Gesetzgebungsverfahren. Eine inhaltliche Bewertung der Neuregelung ist mir daher abschließend noch nicht möglich. Soweit allerdings von Seiten der Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Stellungnahmen abgegeben worden sind, lassen sich diese – verkürzt – wie folgt zusammenfassen: Es ist positiv zu bewerten, dass nunmehr jahrzehntelangen Forderungen der Datenschutzbeauftragten Rechnung getragen wird und eine umfassendere gesetzliche Regelung des Beschäftigtendatenschutzes erfolgt. Es wird sich zeigen müssen, ob sich die gewählte Einfügung der Regelungen des Beschäftigtendatenschutzes in das Bundesdatenschutzgesetz in der Praxis bewähren wird. Bereits aufgrund der zahlreichen Unterschiede zwischen dem Datenschutz im öffentlichen und im nichtöffentlichen Bereich hätte einiges dafür gesprochen, an der ursprünglich beabsichtigten Schaffung eines eigenständigen Beschäftigtendatenschutzgesetzes festzuhalten.

Grundsätzlich ist eine gesetzliche Regelung des Beschäftigtendatenschutzes zu begrüßen, zumal ein angemessener Ausgleich zwischen den Belangen von Arbeitgebern und schutzwürdigen Rechtsgütern der Beschäftigten angesichts vielfältiger widerstreitender Interessen schwierig ist. Allerdings sehe ich mit Blick auf den von der Bundesregierung vorgelegten Gesetzentwurf noch erheblichen Verbesserungsbedarf.

Videoüberwachung zu weitgehend

Zwar soll die heimliche Videoüberwachung durch Arbeitgeber verboten werden, dafür wird jedoch sehr weitgehend eine offene Videoüberwachung zugelassen. Wenn Arbeitgebern nicht jederzeit und an jedem Ort eine offene Videoüberwachung gestattet werden soll, bedarf es einer Konkretisierung der im Gesetzentwurf vorgesehenen Überwachungszwecke. Zudem sollte mit Blick auf die bisherige arbeitsgerichtliche Rechtsprechung die dauerhafte Überwachung von Beschäftigtenarbeitsplätzen untersagt werden.

Des Weiteren lässt der Gesetzentwurf Fragen ungeregelt, die dringend einer Regelung bedürfen: So wird z. B. nicht klargestellt, welche Vorgaben ein Arbeitgeber zu beachten hat, wenn er seinen Arbeitnehmern die private Nutzung von Telekommunikationseinrichtungen gestattet. Dies ist nur ein Beispiel von vielen dafür, wie sehr eine datenschutzrechtlich angemessene Regelung zum betrieblichen Rechtsfrieden beitragen könnte. Vor diesem Hintergrund wird abzuwarten sein, inwieweit den vielfältigen Bedenken im Gesetzgebungsverfahren Rechnung getragen wird.

Weiterführende Informationen:

Stellungnahme des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein zum Regierungsentwurf unter
www.datenschutzzentrum.de/arbeitnehmer/20101012-stellungnahme.html

Einsatz von Ortungssystemen: Permanenter Kontrolldruck unzulässig

Im Berichtszeitraum erreichten mich vermehrt Anfragen von Arbeitnehmern, deren Firmenfahrzeuge mit einem Ortungssystem ausgestattet worden sind. Mit Hilfe eines solchen Systems, in aller Regel über Global Positioning System (GPS), ist es möglich, jederzeit den geographischen Standort des Beschäftigten zu bestimmen und dessen Route nachzuvollziehen.

Die durch den Einsatz eines Ortungssystems veranlasste Erhebung und Verarbeitung personenbezogener Daten, zu denen auch der Aufenthaltsort und das Bewegungsmuster eines Arbeitnehmers zählen, ist nur unter ganz engen Voraussetzungen möglich. Im Rahmen einer Abwägung ist prüfen, ob die Erfassung des Aufenthaltsortes zur Wahrung berechtigter Interessen eines Unternehmens erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Beschäftigten am Ausschluss der Verarbeitung überwiegt. Hierbei ist auch eine Verhältnismäßigkeitsprüfung durchzuführen.

Umfassende Kontrolle verletzt schutzwürdige Interessen

Ortungssysteme zum Zwecke der Optimierung von Fahrzeugeinsätzen (Verringerung von Fahrzeiten zum nächsten Einsatzort) oder zu Logistikzwecken (Verfolgung des Warenstandortes) zu nutzen, kann für ein Unternehmen von großem wirtschaftlichen Nutzen sein. Zu diesen Zwecken eingesetzte Ortungssysteme können grundsätzlich datenschutzrechtlich zulässig sein. Dabei gilt es aber die Grenzen der Verhältnismäßigkeit zu beachten und nicht eine lückenlose Überwachungssituation für den Beschäftigten entstehen zu lassen. Wenn mit Hilfe des Ortungssystems zugleich das Arbeitsverhalten des Beschäftigten (z. B. Dauer von Fahrtunterbrechungen, Verhalten im Straßenverkehr etc.) umfassend kontrolliert wird, er einem permanenten Kontrolldruck ausgesetzt ist, werden seine schutzwürdigen Interessen verletzt. Dies ist datenschutzrechtlich nicht zulässig.

Da mit der Nutzung eines Ortungssystems die Gefahr eines nicht unerheblichen Eingriffs in das Persönlichkeitsrecht des Beschäftigten verbunden ist, ist vor der Einführung solcher Verfahren unter Beteiligung des Betriebsrats der Umgang mit den anfallenden personenbezogenen Daten klar zu regeln: Eine zulässige Datenerhebung erfordert eine konkrete Festlegung der Zwecke des Einsatzes des Ortungssystems. Die Nutzung der Daten zur Verhaltens- und Leistungskontrolle ist ausdrücklich auszuschließen.

Bei Ausgestaltung der Nutzung des Ortungssystems ist der Umgang mit den anfallenden personenbezogenen Daten klar zu regeln.

- Es muss geregelt werden, welche Personen unter Berücksichtigung des Einsatzzwecks Zugriff auf die gespeicherten Daten haben, gegebenenfalls sollte eine Protokollierung des Zugriffs erfolgen.
- Festzuhalten sind die Erfassungshäufigkeit, der Umfang der erhobenen Daten (i. d. R. nur der Standort); vorzusehen sind zeitnahe Löschungsfristen.
- Die Dauer der Speicherung der erhobenen Daten ist auf das für den jeweiligen Zweck erforderliche Maß zu begrenzen.
- Bei der Nutzung des Fahrzeugs zu privaten Fahrten muss das Ortungssystem abschaltbar sein.
- Für den Beschäftigten muss nachvollziehbar sein, welche Daten zu welchen Zwecken bei dem GPS-Einsatz anfallen und wer Zugriff auf diese Daten hat; er muss darüber vom Unternehmen unterrichtet werden.

Schwerpunktprüfung Callcenter: Bislang ohne gravierende Datenschutzverstöße

In den letzten zwei bis drei Jahren mussten wiederholt Bankkunden in Deutschland um ihre persönlichen Daten bangen, weil CDs mit Millionen von vertraulichen Daten wie Namen, Adressen, Geburtsdaten, Telefonnummern und Kontoverbindungen oder auch E-Mailadressen von Callcenter-Mitarbeitern an Dritte weiterverkauft worden sind. Diese Daten sind dann oft zu betrügerischen Zwecken genutzt worden, indem Abbuchungen von Konten erfolgten, ohne dass eine Zahlungsverpflichtung bestand. Unseriöse Firmen verwendeten die Telefonnummern für Anrufe bei tausenden von Bürgerinnen und Bürgern, um ihnen Verträge anzubieten und nach einem zweifelhaften Vertragsabschluss ohne Einzugsermächtigung Geld von deren Bankkonten abzubuchen.

Diese Rechtsverstöße und Skandale haben gezeigt, dass etliche Unternehmen sich ihrer Verantwortung für den Datenschutz ihrer Kunden nicht bewusst sind oder diesen gezielt umgehen. Um am Wirtschaftsleben teilnehmen zu können, müssen Bürgerinnen und Bürger jedoch Adress- und Kontodaten bekanntgeben. Deshalb müssen sie darauf vertrauen können, dass diese Daten geschützt und gesichert sind und bleiben. Gesetzgeber, Aufsichtsbehörden und Unternehmen haben den Auftrag, den Datenschutz für die Betroffenen sicherzustellen.

Da personenbezogene Daten – insbesondere sensible Daten – einen hohen wirtschaftlichen Wert besitzen und ein erhebliches Gefährdungspotential für die Betroffenen darstellen, hatten die Datenschutzbeauftragten des Bundes und der Länder sowie die Verbraucherschützer bereits früh einen dringenden Handlungsbedarf gesehen. Der Bundesgesetzgeber hat daher im Jahr 2009 das Bundesdatenschutzgesetz verschärft und die Regelungen zur Auftragsdatenverarbeitung erheblich strenger gefasst.

Zwar verbessern die Gesetzesänderungen den Standard des Datenschutzes, aber die durch Datenschutzskandale bekannt gewordenen Missbrauchsmöglichkeiten und Defizite lassen sich nicht allein mit gesetzgeberischen Handlungen schließen. Vor diesem Hintergrund habe ich im Bereich der niedersächsischen Callcenter eine Schwerpunktkontrolle durchgeführt.

Die Branche der Callcenter ist sehr heterogen. Es gibt Callcenter, die als interner Dienstleister in einem Konzern tätig und nur für dessen Kunden zuständig sind. Daneben gibt es Callcenter, die mit wenigen Mitarbeiterinnen und Mitarbeitern Aufträge aus der Wirtschaft abarbeiten oder Unternehmen, die mit mehreren hundert Mitarbeitern große Wirtschaftsunternehmen in deren Kundenbetreuung unterstützen.

Foto:
Ben Kraan Architecten BNA

Auch Mitarbeiterdatenschutz geprüft

In mein Prüfkonzept habe ich neben den allgemeinen Fragen zum Datenschutz und zu den technisch-organisatorischen Maßnahmen zu Datenschutz und Datensicherheit nicht nur die Erhebung und Nutzung der Kundendaten, sondern auch den Bereich des Arbeitnehmerdatenschutzes der Callcenter-Beschäftigten aufgenommen. Besonderen Wert habe ich im Rahmen meiner Kontrolle auf die im Unternehmen schriftlich niedergelegten Datenschutzregelungen und deren praktische Umsetzung gelegt. Dies erforderte neben der Prüfung umfangreicher Stellungnahmen der Callcenter immer auch eine Vor-Ort-Prüfung in deren Geschäftsräumen.

Aufgrund der Komplexität der Prüfverfahren sind diese noch nicht alle abgeschlossen. Bei den bisher durchgeführten Kontrollen war festzustellen, dass die geprüften Callcenter eine hohe Bereitschaft zur Zusammenarbeit mit der Datenschutzaufsichtsbehörde zeigten, in einigen Fällen für Anregungen und Hinweise sogar sehr dankbar waren. Ein Zusammenhang zwischen der Größe eines Unternehmens und dessen Datenschutzniveau war nicht zu erkennen. So hatten einige Callcenter sich aufgrund der Anforderungen ihrer Auftraggeber für den Bereich Datenschutz zertifizieren lassen. Sofern sich solche Zertifizierungen auf Selbsteinschätzungen stützten, waren sie allerdings nur bedingt aussagekräftig.

Kontrollen werden fortgesetzt

Vorläufig bleibt festzuhalten, dass der Betrieb eines Callcenters in den weit überwiegenden Fällen im Rahmen der Auftragsdatenverarbeitung stattfand. Dies hatte zur Folge, dass die Verantwortlichkeit für den Datenschutz beim Auftraggeber lag. Durch die neuen Regelungen im § 11 BDSG sind dessen Pflichten verschärft und die Überprüfung der Zuverlässigkeit des beauftragten Callcenters geregelt worden. Insbesondere muss sichergestellt werden, dass die personenbezogenen Daten nicht missbräuchlich durch Mitarbeiter eines Callcenters abgerufen und kopiert werden können. Auch muss der Auftraggeber dafür sorgen, dass alle dem Dienstleister zur Verfügung gestellten und erhobenen Daten nach Abschluss des Auftrags dort gelöscht werden.

Auch wenn ich bisher keine gravierenden Datenschutzverstöße feststellen musste, werde ich die Kontrollen von Callcentern fortsetzen.

Unerwünschte Anrufe gehen meist von Callcentern aus. Dabei hat man es oft mit unverschämten Werbe- und Ausforschungsversuchen zu tun. In solchen Fällen können die folgenden Tipps weiterhelfen:

- Wer ruft an? (Rufnummer notieren)
- Handelt es sich um einen Callcenter-Mitarbeiter?
- Fragen Sie den Anrufer nach seiner Rufnummer, wenn diese nicht im Display angezeigt wird.
- Im Zweifel fragen Sie in der Telefonzentrale der Firma nach.
- Wenn Sie mit Namen angesprochen werden, fragen Sie, woher der Anrufer ihn kennt.
- Bankverbindungen, Geburtsdatum, Vornamen bzw. Adresse nicht am Telefon bekanntgeben.
- Sollte Ihnen Ihre Bankverbindung mitgeteilt werden, damit Sie diese bestätigen, bestreiten Sie die Richtigkeit.
- Nicht notwendige Fragen nicht beantworten („Wozu wollen Sie das wissen?").
- Halten Sie das Gespräch kurz.

Neue Informationspflicht für Unternehmen bei Datenpannen

Seit dem 1. September 2009 verpflichtet der neu eingefügte § 42 a BDSG die verantwortliche Stelle zu unverzüglicher Mitteilung an die Aufsichtsbehörde und die Betroffenen, wenn bestimmte sensiblen Datenarten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und dadurch schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Die Informationspflicht nach § 42 a BDSG soll den Betroffenen vor weiteren Schäden durch möglichen Missbrauch seiner Daten schützen. Soweit die Benachrichtigung der Betroffenen – insbesondere aufgrund der Vielzahl der betroffenen Fälle – einen unverhältnismäßigen Aufwand darstellt, ist stattdessen die Information der Öffentlichkeit durch halbseitige Anzeigen in zwei bundesweit erscheinenden Tageszeitungen vorgesehen. Mir sind seit Einführung dieser Verpflichtung acht Meldungen zugegangen. In drei Fällen bestand tatsächlich eine Meldepflicht, in fünf weiteren konnte letztlich eine Verpflichtung zur Anzeige gem. § 42 a BDSG verneint werden.

Eine Anzeigepflicht lag in folgenden Fällen vor:

- Unter Verneinung einer rechtlichen Verpflichtung teilte ein Unternehmen mit, dass die Konzernrevision aufgrund anonymer Hinweise eine umfangreiche Datensammlung zu Krankeninformationen von fast 600 Mitarbeitern entdeckt habe. Die Daten waren nach Angaben des Unternehmens auf einem Rechner ohne Zugangssperren lokal gespeichert. Die Daten wurden umgehend gelöscht, die betroffenen Führungskräfte vom Bereich Personal „ermahnt“. Aufgrund der sofortigen und umfassenden Löschung war mir eine nähere Aufklärung des Sachverhaltes nicht mehr möglich.
- Ein Versicherungsmakler hatte Versichertendaten (darunter auch Bankverbindungen und Gesundheitsdaten) auf einem Server im Internet unzureichend geschützt gespeichert. Da eine unbefugte Kenntnisnahme nicht ausgeschlossen werden konnte, wurden die Betroffenen über den Vorfall informiert und aufgefordert, ihre Kontobewegungen auf eventuelle Unregelmäßigkeiten zu prüfen.
- Infolge eines Einbruches bei einem Versicherungsvermittler wurden dessen Rechner entwendet. Betroffen waren Gesundheits- und Bankdaten von über 5.000 Versicherungsnehmern. Die Betroffenen wurden über den Vorfall unterrichtet.

In folgenden Fällen lag eine Anzeigepflicht nicht vor:

- Ein Unternehmen meldete, dass ein Auftragsdatenverarbeiter Daten für die Zahlung von Betriebsrenten an einen Unterauftragsdatenverarbeiter weitergegeben habe, obwohl dies explizit ausgeschlossen worden sei.

- Eine Apothekenverrechnungsstelle teilte die Weiterleitung von 24 Rezepten an einen falschen Apotheker mit. Eine schwerwiegende Beeinträchtigung wurde jedoch bereits von der Verrechnungsstelle selbst verneint.
- In einem Unternehmen wurden durch einen Bedienungsfehler zu weitgehende Zugriffsrechte auf Personaldaten innerhalb des Unternehmensnetzwerkes eingeräumt. Hinweise auf erfolgte Zugriffe gab es nicht. Die Mitarbeiter und der Betriebsrat wurden u. a. über die Mitarbeiterzeitung informiert.
- Die Mitarbeiterin einer sozialen Einrichtung stellte Bilder von einem Ausflug von Bewohnern der Einrichtung, auf denen auch deren Behinderung eindeutig zu erkennen ist, bei einem Sozialen Netzwerk ein. Die Bilder wurden von der Mitarbeiterin ohne berufliche Veranlassung angefertigt, ein Personenbezug war jedoch mit hoher Wahrscheinlichkeit nicht herstellbar.
- Im Rahmen einer arbeitsrechtlichen Auseinandersetzung hatte ein an einem Klinikum beschäftigter Arzt 300 Unterlagen von eigenen Patienten sowie Patienten eines weiteren Arztes seinem Rechtsanwalt ungeschwärzt übergeben, der diese ebenfalls ungeschwärzt bei Gericht einreichte. Ich sah keine Gefahr einer schwerwiegenden Beeinträchtigung, da die Unterlagen zu keinem Zeitpunkt Gegenstand der mündlichen öffentlichen Verhandlung waren.

Die Mehrzahl der bisher eingegangenen Meldungen bezogen sich auf Fälle, in denen eine Informationspflicht letztlich zu verneinen war; viele Unternehmen tendierten dazu, im Zweifelsfalle vorsorgliche Meldungen abzugeben, was zu begrüßen ist.

Zusammenfassend ist festzustellen, dass sich die Unternehmen bislang in der Auslegung des neuen § 42 a BDSG nicht sicher waren. Aus diesem Grunde sandten gewissenhafte Betriebe oftmals vorsorglich eine Meldung an mich und überließen mir die Prüfung der Anzeigepflicht. Mit der im Internet zur Verfügung stehenden Hilfestellung zum § 42 a BDSG des Berliner Datenschutzbeauftragten sollte es inzwischen jedoch jedem Unternehmen möglich sein, das Vorliegen der Voraussetzungen selbst zu prüfen.
Die Informationspflicht stellt einen Anreiz für die Unternehmen dar, gewissenhafter mit personenbezogenen Daten umzugehen, weil sie im Falle eines Verstoßes nun nicht nur eventuell ein Bußgeld zu befürchten haben, sondern auch einen öffentlichen Ansehensverlust, wenn die Betroffenen über die Medien informiert werden müssen. Des weiteren erhöht die Informationspflicht das Risiko für die verantwortlichen Stellen, im Falle eines Verstoßes gegen die Vorschriften des BDSG seitens der Betroffenen schadenersatzpflichtig gemacht zu werden, weil es Zweck der Informationspflicht ist, den Betroffenen vor möglichen weiteren Schäden durch Missbrauch seiner Daten zu schützen. Wünschenswert wäre eine solche Verpflichtung auch für öffentliche Stellen, wie sie zum Beispiel in § 18 a des Berliner Datenschutzgesetzes vorgesehen ist.

Weitere Informationen:

Hilfestellung zur Prüfung nach § 42 a BDSG unter
www.datenschutz-berlin.de/content/themen-a-z/informationspflicht-nach-42-a-bdsg

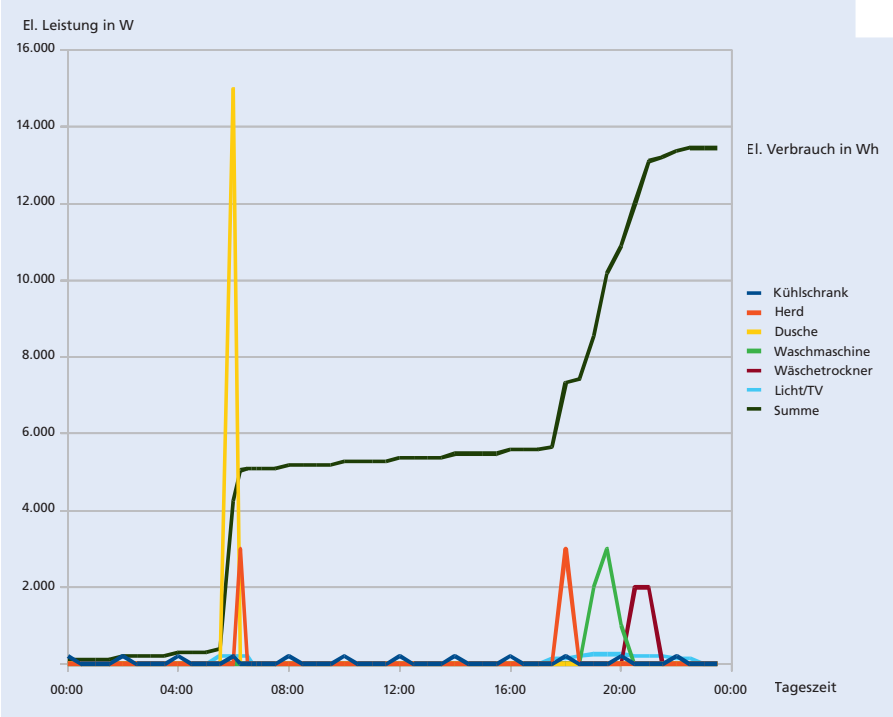
Intelligente Stromnetze: Ich weiß, ob du gestern gekocht hast

Die Frage, ob sich durch intelligente Stromnetze Rückschlüsse auf die Lebensgewohnheiten von Menschen ziehen lassen und wie man dem begegnen kann, wird in Zukunft unter Datenschutzgesichtspunkten eine große Bedeutung erlangen. Es geht um die effiziente Nutzung von Energie durch die Anpassung der Energieversorgung an die tatsächliche Bedarfslage. Damit soll der Diskrepanz zwischen der eingespeisten Energie und dem tatsächlichen Verbrauch begegnet, der Energieverbrauch insgesamt gesenkt und das Klima geschützt werden.

Die Realisierung dieser Ziele hängt davon ab, wie genau der Lastbedarf des Einzelnen zu bestimmten Zeitpunkten ist. Dieser wird künftig durch so genannte intelligente Stromzähler (Smart Meter) gemessen, welche die sekundengenaue Erfassung des Verbrauchs ermöglichen. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können.

Rahmenbedingungen und Ziele

Im Jahr 2007 hat die Europäische Kommission ein Paket von Rechtsvorschriften zum Thema Energie/Klimawandel vorgelegt, das im Ergebnis eine Steigerung der Energieeffizienz um 20 Prozent, eine Reduzierung der Treibhausgasemissionen von 20 Prozent sowie einen Zielwert von 20 Prozent für den Anteil erneuerbarer Energiequellen am Gesamtverbrauch der EU im Jahr 2020 vorsieht. Zur Erreichung dieser Ziele soll insbesondere die Steigerung der Energieeffizienz durch die Nutzung einer Kommunikationsinfrastruktur zum Echtzeit-Informationsaustausch zwischen den Akteuren des Energiemarktes beitragen. Hierdurch soll ermöglicht werden, dass Angebot und Nachfrage zeitnah aufeinander abgestimmt werden.
Die Vorgaben der Kommission sind in Deutschland durch neue gesetzliche Bestimmungen im Energiewirtschaftsgesetz (EnWG) umgesetzt worden, die in einem ersten Schritt seit dem Jahr 2010 bei Neubauten und grundlegenden Renovierungen von Gebäuden den Einbau von Energiezählern vorschreiben, die den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigen. In der Folge werden diese Zähler durch die Anbindung an die Infrastrukturen des Internet auch zur Weitergabe der Messdaten an Mehrwertdienste im Internet genutzt werden können. Ferner sollen Energieversorgungsunternehmen (EVU) ab dem Jahr 2011 den Verbraucherinnen und Verbrauchern einen Stromtarif anbieten, bei dem Anreize zur Energieeinsparung oder zur Steuerung des Energieverbrauchs gegeben werden sollen. Die neuen Zähler müssen diese Tarife abbilden können und die für die Tariffindung relevanten Verbrauchsdaten liefern.
Die Smart Meter sind jedoch nur ein Baustein der angestrebten Energieeffizienzsteigerungen. Eine maßgebliche Rolle wird die wesentlich umfassendere Vision von intelligenten Stromnetzen (Smart Grid) spielen. Denn hier liegt das eigentliche Ziel



Zum Beispiel: Tageslastkurve eines 1-Personen-Haushalts
Quelle: Wikipedia, Trackler

der Vorgaben der Kommission und ihrer Umsetzung im EnWG: Mit den technischen Möglichkeiten des Smart Meters und des Smart Grid soll der Verbrauch so gesteuert werden, dass der Gesamtstromverbrauch reduziert und verstetigt wird. Die positive Folge ist die effektivere Auslastung der Netze und Kraftwerke.
Aber auch die Verbraucherinnen und Verbraucher sollen von der Intelligenz der Stromnetze profitieren. Sie sollen über ihren täglichen Verbrauch informiert werden, möglichst sogar differenziert nach den Strom verbrauchenden Geräten im Haushalt, damit sie entscheiden können, wie und wann sie wie viel Strom verbrauchen und somit ihr Verbrauchsverhalten besser steuern können. Energieeinsparungen im großen Stil werden sich aber erst realisieren lassen, wenn durch einen flächendeckenden Einsatz von Smart Metern als Kontroll- und Steuereinheit die Basis für ein intelligentes Stromnetz gelegt wird, bei dem sich Energie vom Ort der Erzeugung zu jedem beliebigen Punkt verschieben lässt – ähnlich wie Informationen im Internet. Beim Smart Grid gehen das Energiesystem und die Informations- und Kommunikationstechnik (IKT) sozusagen eine Symbiose ein.

Forschungsprojekte und Datenschutz

Zur Unterstützung dieses Wandels bedient sich das Bundesministerium für Wirtschaft und Technologie der Technologie-Förderinitiative „E-Energy“, die Projekte in bundesweit sechs Modellregionen fördert. Die E-Energy-Projekte sollen moderne IKT nutzen, um das Stromversorgungssystem zu optimieren. Eine dieser Modellregionen befindet sich im Raum Cuxhaven und wird von einem überregional tätigen niedersächsischen EVU betreut. Ziel dieses Forschungsprojektes mit dem Namen „eTelligence“ ist es, für die Verbraucher in den an dem Projekt teilnehmen-

Weitere Informationen:
www.e-energy.de
www.etelligence.de

den Haushalten Möglichkeiten der Energie- und Kosteneinsparung und zugleich Potenziale für eine zeitliche Verbrauchsverlagerung zu erschließen. In diesem Zusammenhang sollen der Einsatz und die Effekte der Smart Meter mit angeschlossenen IKT-basierten Feedback-, Informations- und Beratungssystemen sowie teilnahmespezifischen Stromtarifen untersucht und ausgewertet werden.
Ich habe die Implementierung dieses Forschungsprojekts, das zur erfolgreichen Durchführung auf detaillierte Verbrauchsdaten aus den Haushalten angewiesen ist, unter Datenschutzgesichtspunkten beratend begleitet. Hierdurch konnte ein maßgeblicher Beitrag dazu geleistet werden, dass die an dem Projekt teilnehmenden Verbraucherinnen und Verbraucher in geeigneter und transparenter Weise über Zweck und Umfang der bei ihnen erhobenen personenbezogenen Daten informiert werden. Damit ist gewährleistet, dass die Durchführung des Projektes datenschutzkonform auf der Grundlage einer informierten Einwilligung (§ 4 a BDSG) der teilnehmenden Verbraucher erfolgen kann.

Datenschutzrisiken und Anforderungen

Detaillierte Verhaltensprofile bilden Gewohnheiten der Verbraucher ab: Wann wird gefrühstückt, wann gewaschen, wird das Mittagessen lieber auf dem Herd oder in der Mikrowelle zubereitet?

Aber auch über diese konkrete Projektbegleitung hinaus bedürfen künftig der Einsatz von Smart Metern und Smart Grids intensiver datenschutzrechtlicher Begleitung. Wenn – wie möglicherweise nach Abschluss aller E-Energy-Projekte vorgesehen – der Stromverbrauch in jedem einzelnen Haushalt in kurzen Zeitintervallen erfasst werden soll, um einerseits zum Stromsparen anzuregen und andererseits individuelle Tarife anzubieten, so entstehen detaillierte Verhaltensprofile, die die Gewohnheiten der Verbraucherinnen und Verbraucher beim Gebrauch ihrer Wohnung und der Haushaltsgeräte genau abbilden können. Es wäre zum Beispiel vorstellbar, dass die Stromversorger anhand des für bestimmte Geräte typischen Stromverbrauchs zu bestimmten Zeitpunkten erfahren, ob ein Kunde zum Zubereiten des Mittagessens eher den Herd, den Ofen oder die Mikrowelle benutzt. Auch das Ausbleiben des Verbrauchs erlaubt Rückschlüsse auf die Lebensgewohnheiten des Stromkunden: Hat er den Backofen benutzt? Hat er gefrühstückt? Ebenso wären Rückschlüsse auf das Freizeitverhalten möglich: Wann wird der Fernseher eingeschaltet, wann der Computer, wann wird Licht ein- und ausgeschaltet, wie oft wäscht die Geschirrspülmaschine?
Unter datenschutzrechtlichen Gesichtspunkten stellt sich deshalb die Frage, ob eine so hoch aufgelöste und differenzierte Erfassung der Verbrauchsdaten für jeden Haushalt für das Erreichen der Energiesparziele erforderlich ist. Solange es nur darum geht, den Verbrauchern selbst detaillierte Informationen zu ihrem Stromverbrauch zu liefern, ist eine Inhouse-Lösung ausreichend, die die gemessenen Daten nur für den eigenen Computer aufbereitet. Wenn jedoch die zeit- und lastabhängigen Tarife bis auf Haushaltsebene differenziert ausgestaltet werden sollen, dann werden diese Daten nicht in der Wohnung verbleiben können, sondern zur Tarifgestaltung durch das EVU verwendet werden. Hier entstehen datenschutzrechtliche Risiken, mit denen sich auch die DSB-Konferenz im November 2010 befasst und dazu eine Entschließung verabschiedet hat.

Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter www.lfd.niedersachsen.de Pfad: Allgemein > DSB-Konferenzen > Entschließungen

Die Befürchtungen einiger wissenschaftlicher Begleitforscher der E-Energy-Initiative, die Datenschutzbeauftragten könnten die Entwicklung behindern, sind jedoch

unbegründet. Wie die Entschließung der DSB-Konferenz zeigt, geht es nicht darum, technische Entwicklungen zu blockieren, sondern den Prinzipien der strikten Datensparsamkeit und der Datenvermeidung, die im deutschen Datenschutzrecht verankert sind (§ 3 a BDSG), auch bei Smart Grids Geltung zu verschaffen.

Dasselbe gilt für den Einsatz der Smart Meter. Da die Messstellen, die den Anforderungen des § 21 b EnWG entsprechen, wesentlich mehr Verbrauchsdaten des Haushalts anzeigen als bei den alten so genannten Ferraris-Zählern, besteht bei ihnen ein höherer datenschutzrechtlicher Schutzbedarf. Aus diesem Grund müssen technische und organisatorische Maßnahmen nach § 9 BDSG ergriffen werden, um die Kenntnisnahme der angezeigten Daten durch Unbefugte zu verhindern. Sind die Zähler in der Wohnung eingebaut, liegt eine hinreichende Zutrittskontrolle vor, die verhindert, dass sich Unbefugte die Verbrauchsdaten verschaffen. Sind die Zähler jedoch im öffentlich zugänglichen Bereich oder – wie in vielen Wohnanlagen – gesammelt in einem gesonderten Raum untergebracht, zu dem viele Personen Zutritt haben, so müssen Maßnahmen der Zugangskontrolle getroffen werden. Dies können Klappen vor dem Display des Zählers sein, die mit einem individuellen Schlüssel ausgestattet sind. Auch die Abfrage eines PIN-Codes kommt als geeignete Maßnahme der Zugangskontrolle in Betracht.

Ferner sind Maßnahmen zu treffen, die die Datensicherheit bei der Übermittlung der Messergebnisse sicherstellen. Denn zur Bewältigung der anfallenden Datenmengen erlauben Smart Meter das kontaktlose Auslesen der erhobenen Verbrauchsinformationen und die Übermittlung an Sammelstellen über Internet oder Funkverbindung. Bei allen Übertragungen der Messdaten aus der Wohnung oder in die Wohnung ist daher entweder die Anonymisierung oder die Pseudonymisierung der Daten erforderlich. Anderenfalls müssen kryptographische Verschlüsselungsverfahren eingesetzt werden.

Bei allen Übertragungen der Messdaten aus der Wohnung oder in die Wohnung ist entweder die Anonymisierung oder die Pseudonymisierung der Daten erforderlich.

Schließlich müssen auch die Transparenz der Messverfahren und der Datenübermittlung datenschutzrechtlichen Anforderungen genügen. Dies kann nur gewährleistet werden, wenn Ablesezeitpunkte und Ableseintervalle mit dem Betroffenen vertraglich vereinbart werden. Im Übrigen müssen nach der derzeitigen datenschutzrechtlichen Rechtslage weitere Angebote, die über die gesetzlichen Anforderungen hinaus gehen, gesondert vertraglich geregelt werden. Es bedarf also auch insoweit einer Einwilligung i. S. d. § 4 a BDSG durch den Betroffenen. Dies gilt insbesondere dann, wenn Lastprofile bei Messungen mit kurzen Intervallen auf zentrale Rechner übertragen werden sollen, damit die Betroffenen sie über das Internet abrufen können.

Erfreulicherweise konnte ich durch meine Begleitung des Forschungsprojektes „eTelligence“ sicherstellen, dass diese technisch-organisatorischen und vertraglichen Anforderungen des Datenschutzes bei der Projektdurchführung beachtet werden.

Vereine:
Sensibilität für Datenschutz gestiegen

Zur Gestaltung eines aktiven Vereinslebens ist die effiziente Nutzung personenbezogener Daten der Vereinsmitglieder unerlässlich. Für die Einbindung der Mitglieder in Entscheidungsprozesse der Vereinsgremien wird dabei unabhängig von der Vereinsgröße mittlerweile ebenso selbstverständlich auf die aktuellen Kommunikationstechniken von Internet und E-Mail zurückgegriffen wie bei der Darstellung von Vereinsaktivitäten oder neuen Angeboten.

Das Verständnis und die Sensibilität für die dabei auftretenden Datenschutzfragen ist in den letzten Jahren erfreulicherweise sowohl bei den Vereinsverantwortlichen wie auch bei betroffenen Vereinsmitgliedern deutlich gestiegen. Damit einher geht eine gestiegene Zahl von Anfragen an mich rund um das Thema Datenschutz im Verein. Typische Fragen beziehen sich dabei z. B. auf

- den zulässigen Umfang der Datenverarbeitung im Rahmen der Vereinsmitgliedschaft,
- die Übermittlung von Mitgliederdaten (z. B. Mitgliederlisten) an andere Vereinsmitglieder, Dachorganisationen oder an die Medien,
- die Übermittlung von Mitgliederdaten an Wirtschaftsunternehmen (z. B. an Versicherungsunternehmen im Rahmen von Gruppenversicherungsverträgen) oder an Sponsoren,
- technisch-organisatorische Anforderungen bei der Verwaltung der Mitgliederdaten oder
- den Umgang mit Veröffentlichungen im Internet allgemein.

Zur Beantwortung dieser klassischen Fragestellungen und als Service für alle Interessierten halte ich daher auf meiner Internetseite unter dem Thema „Vereine“ eine umfassende Information als PDF-Datei zum Download bereit.

Weitere Informationen:

zum Datenschutz in Vereinen unter www.lfd.niedersachsen.de
Pfad: Themen > Vereine

Sportler-Datenschutz: Veröffentlichung von Sanktionen unzulässig

Einen Schwerpunkt meiner Beratungstätigkeit im Berichtszeitraum bildeten Internet-Veröffentlichungen von Vereins- und Verbandssanktionen wie Spielersperren und Startverbote insbesondere im Zusammenhang mit der Dopingbekämpfung im Sport.

Die Veröffentlichung von Sportgerichtsentscheidungen im Internet mit Nennung des Sportlernamens stellt eine Übermittlung personenbezogener Daten an Dritte i. S. d. § 3 Abs.4 Nr.3b BDSG dar. Jede Übermittlung solcher Daten an Dritte beinhaltet einen Eingriff in das allgemeine Persönlichkeitsrecht des betroffenen Sportlers, der für seine Zulässigkeit einer gesetzlichen Grundlage bedarf. Eine solche steht jedoch nicht zur Verfügung, insbesondere gibt es keinen Erlaubnistatbestand nach dem BDSG. Etwaige Satzungs- oder Verbandsregelungen (z. B. unter Bezugnahme auf den entsprechenden Kodex der Nationalen Anti Doping Agentur – NADA –) reichen zur Rechtfertigung eines solchen Eingriffs jedenfalls nicht aus. Denn mit einer Veröffentlichung im Internet ist nicht nur ein weltweiter Zugriff auf die Daten, sondern darüber hinaus vor allem eine elektronische Recherchierbarkeit möglich, welche es jedem Internet-Nutzer jederzeit erlaubt, durch die Eingabe des Namens des Betroffenen in eine Suchmaschine sämtliche zu dieser Person vorhandenen Angaben zu sammeln und zur Erstellung eines Persönlichkeitsprofils zu nutzen.

Zwar sollen durch die Veröffentlichung sportgerichtlicher Entscheidungen, auch soweit sie mit dem Namen des betroffenen Sportlers erfolgen, neben spezialauch generalpräventive Ziele erreicht werden, was grundsätzlich legitim ist. Dafür ist deren Veröffentlichung im Internet jedoch nicht erforderlich. Ausreichend ist vielmehr, dass entsprechende Sanktionen nur vereins- oder verbandsintern publiziert werden, z. B. in nur für verantwortliche Personen einsehbare Publikationen oder durch eine Veröffentlichung der Sanktionen in einem zugriffgeschützten Intranetforum.

Unter Datenschutzgesichtspunkten ist daher die zumeist von Sportverbänden geübte Praxis der vollständigen Publizierung ihrer gegen einzelne Sportler verhängten Sanktionen im Internet unzulässig. Zu diesem Ergebnis gelangte auch der so genannte Düsseldorfer Kreis (ein Gremium der Datenschutzbeauftragten des Bundes und der Länder für den nicht-öffentlichen Bereich), der in seiner Sitzung im November 2009 einen entsprechenden Beschluss gefasst hat.

Beschluss des Düsseldorfer Kreises unter: www.lfd.niedersachsen.de Pfad: Unser Netzwerk > Düsseldorfer Kreis > 27.11.2009

Unzulässig: Starterlaubnis nur bei Einwilligung in Datenveröffentlichung

Eine Reihe von Anfragen, die mich erreichten, betrafen die Frage nach der Zulässigkeit der Veröffentlichung von Spiel- und Wettkampfergebnissen im Internet oder anderen Publikationen. Dabei war auch zu beobachten, dass Sportverbände auf Bundes- oder Landesebene zunehmend von den Mitgliedsvereinen bei

Meldung ihrer Mannschaften oder einzelner Sportler zu Sportwettkämpfen oder Punktspielen verlangen, dass die Sportler in die Veröffentlichung ihrer wettkampfrelevanten Daten im Internet und anderen Medien einwilligen und von der Einwilligung deren Starterlaubnis abhängig gemacht wird. Dieses Einwilligungsverlangen wird auch damit begründet, dass immer häufiger Sportler fordern, dass die von ihnen erzielten Ergebnisse aus dem Internet entfernt werden.
Unter Datenschutzgesichtspunkten ist diese Praxis unzulässig. Die Erteilung einer solchen Einwilligung, von der die Zulassung zur Wettkampfteilnahme oder zum Punktspielbetrieb abhängt, erfolgt zumeist nicht freiwillig i. S. d. § 4 a BDSG und ist daher datenschutzrechtlich unwirksam.
Die Zulässigkeit der Veröffentlichung von Spiel- bzw. Wettkampfergebnissen oder Ranglisten mit den Namen der Sportlerinnen und Sportler im Internet oder anderen Medien durch den veranstaltenden Sportverband richtet sich daher nach § 28 Abs. 1 Nr. 3 BDSG. Danach ist eine Veröffentlichung von allgemein zugänglichen Daten allerdings zulässig, sofern nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veröffentlichung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.
Die von einem Sportverein oder vom Verband ausgerichteten Spiele bzw. Wettkämpfe sind regelmäßig öffentlich (Ausnahmen bei so genannten Randsportarten sind aber denkbar). Zudem wissen und wünschen die antretenden Sportlerinnen und Sportler, dass die Wettkämpfe oder Punktspiele in der Öffentlichkeit ausgetragen werden und darüber auch berichtet wird. Somit dürfen die dort öffentlich bekannt gegebenen Daten der Sportlerinnen und Sportler als allgemein zugängliche Daten auch im Internet veröffentlicht werden. Zu diesen Daten zählen:

- Vorname und Name,
- Geschlecht,
- Geburtsjahr,
- Spiel- bzw. Wettkampfergebnis und Bilanz (Rangliste),
- Verein,
- Mannschaft.

Darüber hinaus gehende Daten, wie z. B. Nationalität, Geburtsdatum oder Adresse werden jedoch nicht im Rahmen der vom Verein oder Verband ausgerichteten Sportveranstaltungen öffentlich bekannt gegeben. Diese Daten sind daher nicht allgemein zugänglich und dürfen nur mit einer freiwilligen Einwilligung des betroffenen Sportlers im Internet oder in anderen Medien veröffentlicht werden.
In meiner Beratungspraxis vertrete ich daher die Auffassung, dass bei Beachtung dieser Maßgaben die Veröffentlichungen von Spiel- und Wettkampfergebnissen mit den personenbezogenen Daten der Sportlerinnen und Sportler, die diese Ergebnisse erzielt haben, datenschutzrechtlich nicht zu beanstanden sind.

Paradigmenwechsel:
Adresshandel nur noch mit Einwilligung zulässig

Bei der Verarbeitung personenbezogener Daten zum Zwecke des Adresshandels geht es um Datenverarbeitungsprozesse von Dienstleistern mit dem Ziel der geschäftsmäßigen Übermittlung von Adressdaten, die im Bundesdatenschutzgesetz (BDSG) in § 29 geregelt sind. Daneben regelt § 28 Abs. 3 BDSG, unter welchen Voraussetzungen Adressdaten zur Werbung für eigene oder fremde Angebote verarbeitet oder genutzt werden dürfen.

Galten früher Adresshandel und Werbung als die zwei Seiten derselben Medaille, so stehen beide Verarbeitungsgebiete nach meiner Auffassung sowie der überwiegenden Ansicht in der Fachliteratur seit der BDSG-Novelle separat nebeneinander. Dies folgt daraus, dass nach § 28 Abs. 3 Satz 2 BDSG ohne Einwilligung des Betroffenen listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe nunmehr nur für die

- Werbung für eigene Angebote,
- Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen,
- Einwerbung von Spenden

genutzt werden dürfen. Schließlich ist die neu gefasste gesetzliche Erlaubnis in § 28 Abs. 3 BDSG auf die Übermittlung von Daten für Zwecke der Werbung im Allgemeinen und die Hinzuspeicherung weiterer Daten für die Werbung zu eigenen Angeboten im Besonderen beschränkt. Es handelt sich also um die klassische Werbung begünstigende Ausnahmen von dem nunmehr in § 28 Abs. 3 Satz 1 BDSG festgelegten Grundsatz, dass die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung nur aufgrund einer Einwilligung des Betroffenen zulässig ist.

Klassischer Adresshandel nicht mehr privilegiert

Nur Unternehmen, die die Adressdaten ihrer Kundschaft ursprünglich zu vertraglichen Zwecken erhoben und verarbeitet haben, können diese Daten nach § 28 Abs. 3 BDSG weiterhin sowohl zur Werbung für eigene Angebote nutzen als auch an andere Unternehmen, die diese wiederum zu Werbezwecken nutzen wollen, veräußern, ohne dass sie dafür der Einwilligung des Betroffenen bedürfen. Die Tätigkeit des Adresshandels dagegen, der als Gewerbe selbst keine Werbung betreibt, sondern den werbenden Unternehmen Adressdaten für deren werbliche Zwecke zuliefert, ist nach § 29 BDSG als der für den Adresshandel einschlägigen Spezialvorschrift zu beurteilen. Folglich ist der mit der BDSG-Novelle in § 29 Abs. 1 Satz 2 und Abs. 2 Satz 2 neu eingefügte Hinweis auf § 28 Abs. 3 von Bedeutung, wonach der Adresshandel nur noch aufgrund freiwilliger und informierter Einwilligung des Betroffenen zulässig ist.
Der Gesetzgeber hat also die selbst werbenden oder mit ihren selbst erhobenen Adressdaten handelnden Unternehmen deutlich privilegiert gegenüber reinen Adresshandelsunternehmen. Mit der Neufassung der einschlägigen Bestimmungen ist folglich ein Paradigmenwechsel im Bereich des Adresshandels mit der Folge einher gegangen, dass

- dieser in jedem Fall nur noch mit Einwilligung des Betroffenen in die automatisierte Verarbeitung und Übermittlung personenbezogener Daten zulässig ist (so genanntes Opt-in) und
- eine Zuspeicherung von Daten aus anderen Quellen unzulässig ist.

An die für Werbezwecke zugelassene Übermittlung von Adressdaten ist darüber hinaus die Pflicht der übermittelnden Stelle geknüpft, für die Dauer von zwei Jahren ab der Übermittlung den Empfänger und (lückenlos) die Herkunft der übermittelten Daten zu speichern, um dem Betroffenen auf Verlangen hierüber Auskunft erteilen zu können. Auch der neue Empfänger der Adressdaten muss eine entsprechende Speicherung über den Erhalt und die „Vorbesitzer" der Daten vornehmen und zusätzlich – zumindest bei der ersten Datennutzung zur werblichen Ansprache nach Datenübernahme – die Stelle eindeutig in seinem Werbemedium hervorheben, die die Daten erstmalig erhoben hat.

Auskunfteien: BDSG-Novelle bringt geforderte Einschränkungen

Das Bundesdatenschutzgesetz (BDSG) ist auch auf dem Gebiet der automatisierten Verarbeitung personenbezogener Daten in Zusammenhang mit der Beauskunftung durch Wirtschafts- und Handelsauskunfteien novelliert worden.

Besonders hervorzuheben sind hier:

- die gesetzliche Einschränkung der Datenübermittlung an Auskunfteien bei bestehenden Forderungen und die gesetzliche Regelung der Übermittlungen bei Bankgeschäften (§ 28 a BDSG, gilt seit 01.04.2010),
- die Vorgabe, hinsichtlich der bereits bislang bestehenden Pflicht, Auskünfte nur bei glaubhafter Darlegung eines berechtigten Interesses erteilen zu dürfen, nunmehr hierzu Stichprobenverfahren und in diesem Rahmen einzelfallbezogene Überprüfungen durchführen zu müssen (§ 29 Abs. 2 BDSG, gilt seit 01.04.2010),
- die Festlegung von Regeln für das im Lebensalltag immer relevanter werdende Scoring (§ 28 b BDSG, gilt seit 01.04.2010),
- die Ausweitung der auch in diesem Zusammenhang bestehenden Auskunftsrechte (§ 34 Abs. 2 ff BDSG, gilt seit 01.04.2010).

Gesetzliche Einschränkung der Datenübermittlung

Das BDSG erkannte auch schon bisher grundsätzlich das Bedürfnis an, dass zum Schutz vor Kreditbetrug und Zahlungsausfällen relevante und zutreffende personenbezogene Daten der am Wirtschaftsleben teilnehmenden Bürgerinnen und Bürger an Auskunfteien übermittelt und von diesen gespeichert werden dürfen (z. B. Negativmerkmale aus öffentlichen Schuldnerverzeichnissen, Informationen zum Zahlungsverhalten, Kreditverträge), ohne dass eine Einwilligung von dem Betroffenen einzuholen oder dieser über die Speicherung zu informieren wäre.

Die BDSG-Novelle hat insoweit die – von den Datenschutzaufsichtsbehörden schon länger vertretene – Klarstellung gebracht, dass nunmehr Daten über eine Forderung an Auskunfteien nur noch übermittelt und von dieser auch nur noch an berechtigte Dritte beauskunftet werden dürfen, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und mindestens eine der folgenden fünf Voraussetzungen gegeben ist:

1. Der Betroffene hat die Forderung ausdrücklich anerkannt.
2. Der Betroffene hat die Forderung nicht bestritten und wurde nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt, wobei
   - zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen müssen und
   - die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat.

3. Das der Forderung zugrunde liegende Vertragsverhältnis kann aufgrund von Zahlungsrückständen fristlos gekündigt werden, und die verantwortliche Stelle hat den Betroffenen über die bevorstehende Übermittlung unterrichtet.
4. Die Forderung wurde durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt, oder es liegt ein Schuldtitel nach § 794 Zivilprozessordnung vor.
5. Die Forderung ist nach § 178 Insolvenzordnung festgestellt worden und wurde vom Schuldner im Prüfungstermin nicht bestritten.

Auch der neue § 28a Abs.1 BDSG sieht jedoch in den Fällen von anerkannten oder titulierten Forderungen keine vorherige Information des Schuldners über die bevorstehende Einmeldung der Forderung durch den Gläubiger bei einer Auskunftei vor.
Da die Vertragspartner der Auskunftei nur dann ein berechtigtes Interesse an der Information über die Nichterfüllung einer Forderung haben, wenn diese auf Zahlungsunfähigkeit oder Zahlungsunwilligkeit beruht, hat der Gesetzgeber zudem die Einräumung zusätzlicher „nachgehender Karenzzeiten" aufgrund des in der Regel bereits längeren Vorverfahrens zu Recht nicht als notwendig angesehen (siehe auch Stellungnahme der Bundesregierung im Gesetzgebungsverfahren, BT-Drucksache 16/10581, Seite 2).

Gesetzliche Regelung der Übermittlungen zu Bankgeschäften

Die in der Vergangenheit üblichen Vereinbarungen zwischen Kunden und Kreditinstituten zur Mitteilung von Informationen an Auskunfteien (so genannte Schufa-Klauseln) sind durch die BDSG-Novelle obsolet geworden. Kreditinstitute dürfen jetzt personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung von Vertragsverhältnissen (nur) zu bestimmten Bankgeschäften an Auskunfteien übermitteln. Der Betroffene ist vor Abschluss des Vertrages hierüber jedoch zu unterrichten.
Der früher geübten – datenschutzrechtlich umstrittenen – Praxis, Daten betroffener Kunden bereits im Rahmen vorvertraglicher Verhandlungen zur Herstellung von Markttransparenz (so genannte Konditionenanfragen) bei Auskunfteien einzumelden, ist mit der BDSG-Novelle nunmehr der Boden entzogen. Auch mit Einwilligung der Betroffenen dürfen jetzt im Rahmen von Konditionenanfragen erlangte Kundendaten weder an Auskunfteien übermittelt, noch von Auskunfteien erhoben oder gespeichert und auch nicht an Dritte beauskunftet werden.

Neue Nachmeldepflicht

Neu ist auch, dass in allen Fällen, in denen Einmeldungen von Daten zu bestehenden Forderungen oder zu Bankgeschäften an Auskunfteien erfolgt sind, die jeweils verantwortliche Stelle verpflichtet ist, nachträgliche Änderungen der zugrunde liegenden Tatsachen der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Verletzung der Mitteilungspflichten kann jetzt als Ordnungswidrigkeit mit einem Bußgeld bis 50.000 Euro geahndet werden.

Auskünfte nur bei glaubhafter Darlegung eines berechtigten Interesses

Das für die Erlangung einer Wirtschaftsauskunft u.a. erforderliche „berechtigte Interesse" an der Auskunft liegt nur dann vor, wenn ein Vertragspartner im Falle des Abschlusses des geplanten Geschäfts ein finanzielles Ausfallrisiko eingeht. Dies ist dann der Fall, wenn er z.B. gegenüber dem anderen Vertragspartner nicht unerhebliche Vorleistungen erbringt oder es sich um Bestellung/Lieferung auf Rechnung, Ratenkauf, Kreditvergabe, Leasinggeschäfte, Mietverträge oder sonstige Verträge mit kreditorischen Risiken handelt.
Dass der Abschluss von Verträgen solchen Inhalts ernsthaft und unmittelbar bevorsteht, musste schon bisher vom Anfragenden glaubhaft konkret und für die Auskunftei erkennbar angegeben werden. Nun ist jedoch die gesetzliche Verpflichtung der Auskunftei hinzu gekommen, ein geeignetes Stichprobenverfahren zu entwerfen und anzuwenden, aufgrund dessen die Stichproben-Fälle von der Auskunftei detailliert hinsichtlich des berechtigten Interesses überprüft werden müssen. Der Anfragende unterliegt der Verpflichtung zur Mitwirkung an der Überprüfung aufgrund seiner gesetzlichen Pflicht zur Darlegung des berechtigten Interesses.

Bonitätsabfragen durch die Wohnungswirtschaft

Schon seit längerem ist es gängige Praxis, dass sich Vermieter durch Anfragen bei Wirtschaftsauskunfteien Klarheit über die Bonität potentieller Mieter verschaffen wollen, um Mietausfälle oder den Vertragsschluss mit so genannten Mietnomaden zu vermeiden. In Anerkennung des berechtigten Interesses beider Seiten haben die Aufsichtsbehörden für den Datenschutz im Oktober 2009 ihre Auffassung zu den datenschutzrechtlichen Voraussetzungen solcher Anfragen in einem Beschluss veröffentlicht. Danach gelten folgende Anforderungen:

1. Vermieter dürfen erst dann eine Auskunft zu einem Mietinteressenten einholen, wenn der Abschluss des Mietvertrags mit diesem Bewerber nur noch vom positiven Ergebnis einer Bonitätsprüfung abhängt.
2. Es dürfen nur folgende Datenkategorien nach Darlegung eines konkreten berechtigten Interesses an Vermieter übermittelt werden, sofern diese Daten zulässigerweise an die Auskunftei übermittelt oder von dieser erhoben wurden:
   - Informationen aus öffentlichen Schuldner- und Insolvenzverzeichnissen oder
   - sonstige Daten über negatives Zahlungsverhalten zu noch offenen oder solchen Forderungen, deren Erledigung nicht länger als ein Jahr zurückliegt und
   - eine Bagatellgrenze von insgesamt 1.500 Euro überschritten wird.
3. Die Übermittlung von Scorewerten an Vermieter ist unzulässig, sofern darin andere als die unter Nummer 2 erwähnten Daten verwendet werden.
4. Vermieter dürfen weitergehende als die unter 2. genannten Daten grundsätzlich auch nicht im Wege einer Einwilligung oder einer Selbstauskunft des Mietinteressenten von einer Auskunftei erheben.

Der Beschluss ist vollständig einsehbar unter:
www.lfd.niedersachsen.de
Pfad: Unser Netzwerk >
Düsseldorfer Kreis >
22.10.2009

Scoring

Viele Auskunfteien bilden über die in ihren Dateien geführten Betroffenen Scorewerte, die sie an ihre abfragenden Kunden übermitteln. Kunden sind neben Kredit- und Versicherungsunternehmen u. a. auch Unternehmen der Telekommunikation oder des Versandhandels. Der jeweilige Scorewert, auch Bonitätsindex genannt, stellt einen Richtwert dar, mit welcher Wahrscheinlichkeit ein Vertrag insbesondere bei wiederkehrende Zahlungen vom jeweiligen Kunden ohne Ausfall erfüllt werden wird. Dieser Wert stellt im Wirtschaftsleben einen maßgeblichen Entscheidungsparameter, z. B. über die Gewährung eines Kredites, dar. Allerdings bestand bisher Unklarheit darüber, wie bzw. unter Verwendung welcher Basisdaten dieser Wert von den Auskunfteien ermittelt wurde. Die konkrete Beantwortung entsprechender Fragen wurde zumeist mit dem Hinweis auf „das Geschäftsgeheimnis“ vermieden.
Mit der Novelle zum BDSG hat der Gesetzgeber im neuen § 28 b erste Vorgaben dazu geschaffen, welche Voraussetzungen bei der Bildung von Scorewerten ab 01.04.2010 einzuhalten sind.
Danach darf ein Wahrscheinlichkeitswert nur zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind und
2. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden, wobei im Falle der Nutzung (auch) von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser (so genannten Geo-)Daten zu unterrichten ist.

Bei der Verwendung des Scorewerts sind im Falle einer ablehnenden Entscheidung dem Betroffenen der diesbezügliche Zusammenhang aufzuzeigen und auf Verlangen die wesentlichen Gründe dieser Entscheidung mitzuteilen und zu erläutern.
Leider hat der Gesetzgeber nicht die Daten im Einzelnen aufgeführt, die für die Berechnung des Wahrscheinlichkeitswerts zugrunde gelegt werden dürfen bzw. müssen. Sie müssen lediglich nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sein. In einem Bericht „Verbraucherinformation Scoring“, der im Auftrag des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz erstellt und im Juni 2009 veröffentlicht wurde, sind eklatante Mängel bei der Scorebildung dargestellt, die große Schwierigkeiten der Auskunfteien vermuten lassen, sich den wissenschaftlichen Anforderungen zu nähern, die seit dem Jahr 2010 Voraussetzung für die Beauskunftung von Scorewerten sind.

Der Bericht „Verbraucherinformation Scoring“ ist abrufbar unter: www.bmelv.de/cae/servlet/contentblob/638114/publicationFile/36026/Scoring.pdf

Insofern werde ich mich auch künftig mit dieser Thematik befassen müssen. Im Dialog mit den Auskunfteien wird herauszuarbeiten sein, worüber mit welchen Daten Scorewerte datenschutzkonform gebildet werden dürfen und inwieweit das von den Auskunfteien immer noch vorgetragene Argument des Geschäftsgeheimnisses weitestgehende Einschränkung durch die gleichermaßen geltenden Grundsätze der Wissenschaftlichkeit erfährt.

Rechte der Betroffenen auf Auskunft

Über die bisherige Regelung in § 34 Abs. 1 BDSG hinaus, wonach die jeweilige verantwortliche Stelle – und damit auch Auskunfteien – dem Betroffenen auf dessen Verlangen Auskunft zu erteilen hat

1. über zu seiner Person gespeicherte Daten,
2. woher die Daten bezogen wurden,
3. an wen die Daten weitergegeben werden und
4. zu welchem Zweck sie gespeichert wurden,

ist aufgrund der BDSG-Novelle jetzt auch in jedem Fall – also auch durch andere Stellen als Auskunfteien, insbesondere Kreditinstitute – bei Verwendung eines Wahrscheinlichkeitswerts von der für die Entscheidung verantwortlichen Stelle Auskunft zu erteilen über

1. die innerhalb der letzten sechs Monate vor Antragstellung erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte und
2 die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten. Darüber hinaus muss den Betroffenen
3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form erläutert werden.

Ergänzend gilt im Fall der Scorewertbildung durch Auskunfteien, dass sie dem Betroffenen Auskunft zu erteilen haben über

1. die innerhalb der letzten zwölf Monate vor Antragstellung übermittelten Scorewerte sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind, und
2. die sich zum Zeitpunkt des Auskunftsverlangens nach den von der verantwortlichen Stelle zur Berechnung angewandten Verfahren ergebenden aktuellen Wahrscheinlichkeitswerte.

Jede Auskunft unentgeltlich

Der Gesetzgeber hat auch für die Kosten der Auskunftserteilung eine Neuregelung getroffen. Grundsätzlich war die Auskunft bereits nach dem alten Recht unentgeltlich. Etwas anderes galt, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen konnte. Diese Ausnahmeregelung wurde zumindest von einer Auskunftei zum Anlass genommen, generell Geld für eine schriftliche Auskunft zu verlangen. Zudem blieb für den Betroffenen undurchsichtig, wie sich die Kosten für sein Auskunftsersuchen errechnen.
Mit der Neuregelung ist zunächst jede Auskunft unentgeltlich zu erteilen. Für Auskunfteien gilt, dass der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen kann. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Für die Berechnung des Entgelts wurde jetzt klarer geregelt, dass es über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen darf. Weiterhin wurde klargestellt, dass ein Entgelt nicht verlangt werden darf, wenn besondere Umstände die Annahme rechtfertigten, dass Daten unrichtig oder unzulässig gespeichert werden, oder die eingeholte Auskunft ergibt, dass die Daten zu berichtigen oder zu löschen sind.

Bislang wurden von den Auskunfteien in den Auskünften nur pauschal angegeben, dass sich darin Schätzdaten befinden können. Nunmehr sind sie vom Gesetzgeber verpflichtet worden, konkret anzugeben, bei welchen der zur Scorewertbildung genutzten Daten es sich um Schätzdaten handelt. Ebenso konnten Auskunfteien ihrer Kundschaft (z. B. Kreditinstituten) bisher mitteilen, dass über die Betroffenen gesperrte Daten vorliegen. Dies ist nun nach § 35 Abs. 4a BDSG rechtswidrig. Die Auskunft darf weder die Tatsache der Sperrung noch Hinweise auf eine Sperrung enthalten. Die Befürchtung von Auskunfteien, dass diese Regelung zu Missbräuchen führen kann, ist nicht begründet, da ein Bestreiten nur dann zur Sperrung von Daten führt, wenn das Bestreiten nicht gegen die Grundsätze von Treu und Glauben verstößt.

Legitimation durch Ausweiskopie?

Auskunftserteilung erst nach Vorlage einer Ausweiskopie nur noch in konkreten Zweifelsfällen, z.B. bei sonst drohender Namensverwechselung.

Abschließend soll hier noch das in der datenschutzaufsichtlichen Praxis kontrovers diskutierte Thema der Legitimation des Auskunft Verlangenden durch Vorlage einer Ausweiskopie berichtet werden:
Eine Reihe von Aufsichtsbehörden hatte bisher im Interesse des Datenschutzes eine solche Legitimation befürwortet. Die Praxis hat jedoch gezeigt, dass dieses Verfahren wegen des damit verbundenen zeitlichen, organisatorischen und finanziellen Aufwandes für den Anfragenden in der Regel als zu aufwändig und nicht erforderlich anzusehen ist. Im Zweifel führt eine solche Legitimationsforderung dazu, dass der Bürger auf die Geltendmachung seines Auskunftsrechts verzichtet. Deshalb vertreten die Aufsichtsbehörden auch aufgrund meines entsprechenden Vorstoßes nunmehr die Ansicht, dass die Auskunftserteilung erst nach Vorlage einer Ausweiskopie nur noch in konkreten Zweifelsfällen, z. B. bei sonst drohender Namensverwechselung in Betracht kommen kann.

Datenschutz in Telemedien: Bedenkliche Defizite bei der Kenntnis von Rechten und Pflichten

Ich bin als zuständige Aufsichtsbehörde auch für die Einhaltung der datenschutzrechtlichen Bestimmungen nach dem Telemediengesetz (TMG) für Telemedien zuständig, deren Betreiber ihren Sitz in Niedersachsen haben.

Nach Zahlen des Landesbetriebs für Statistik und Kommunikationstechnologie Niedersachsen (Niedersachsen-Monitor 2010, Seite 46) betrug die Anzahl der in Niedersachsen im Jahr 2009 registrierten Internet-Domains 997.767 und deutschlandweit 11.995.914. Weltweit waren 2008 nach Angaben des US-amerikanischen Unternehmens VeriSign etwa 177 Millionen Domains gelistet. Auch wenn diese Zahlen in keine Relation zur tatsächlichen Nachfrage und Nutzung der angebotenen Telemedien gesetzt wurden, gelten, zumindest statistisch, für über sechs Prozent der weltweiten Internetseiten deutsche Datenschutzbestimmungen. In der Praxis zeigte sich allerdings, dass sich eine große Anzahl der Eingaben auf Anbieter von Telemedien außerhalb unseres Zuständigkeitsbereichs bezogen. Dies betraf insbesondere die Direktmarketing-Branche und soziale Netzwerke.

Übermittlung von IP-Adressen ohne Einwilligung oft unzulässig

Der Schwerpunkt der im Berichtszeitraum in Niedersachsen eingegangenen Eingaben zum Datenschutz in Telemedien betraf die Themenfelder soziale Netwerke, Internet-Foren, Direktmarketing sowie den Internetdienst Google Street View. Bei der Prüfung von Verstößen gegen den Datenschutz bei Telemedien musste ich leider feststellen, dass nur wenige Bürger ihre Betroffenenrechte wirklich kennen. Aber auch bei den Telemedien-Anbietern gab es bedenkliche Defizite bei der Kenntnis von Rechten und Pflichten, die sich aus dem Umgang mit personenbezogenen Daten ergeben.
Ebenso fehlte es regelmäßig an der Fachkunde, Telemedien im Sinne der Informationssicherheit sicher zu gestalten. Oft wurde angenommen, dass eine Software „von Haus aus“ nicht nur sicher, sondern auch datenschutzrechtlich unbedenklich sei, wenn sie nur oft genug im Internet verwendet wird. Dass auch auf der eigenen Webseite eingebundene Werbung oder Reichweitenmessung ein Bußgeldtatbestand sein kann, war kaum bekannt. Insbesondere der Webseitenbetreiber, der ohne konkrete Einwilligung der Nutzer deren personenbezogene Daten, wie z. B. die IP-Adresse, über Dienste wie Google Analytics, Google AdSense oder Facebooks Like-It-Button in die USA übermittelt, muss in der Regel mit einem Bußgeld rechnen. Um hier Abhilfe zu schaffen, habe ich im November 2010 eine Handreichung für Anbieter von Telemedien veröffentlicht (siehe Hinweis am Ende des Artikels).

Was sind Telemedien?
Telemedien sind nach § 1 Telemediengesetz (TMG) alle elektronischen Informations- und Kommunikationsdienste, die weder Rundfunk noch reine Telekommunikationsdienste oder telekommunikationsgestützte Dienste (§ 3 Nr. 24 und 25 Telekommunikationsgesetz – TKG –) sind. Die Abgrenzung kann im Einzelfall schwierig sein. Telemediendienste sind zum Beispiel :

- Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit
- Video auf Abruf, soweit es sich nicht nach Form und Inhalt um einen Fernsehdienst im Sinne der Richtlinie 89/552/EWG handelt,
- Online-Dienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen
- die kommerzielle Verbreitung von Informationen über Waren-/Dienstleistungsangebote mit elektronischer Post.

Datenschutzverstöße in sozialen Netzwerken und Internet-Foren

Ein nicht unwesentlicher Anteil der Eingaben zu Datenschutzverstößen in sozialen Netzwerken und Foren betraf Dienstleister, die ihren Sitz nicht in Deutschland hatten und somit auch nicht unter das deutsche Datenschutzrecht fielen. Insbesondere die Dienstleistungen von US-amerikanischen Unternehmen werden von der Mehrheit der deutschen Bevölkerung angenommen, offenbar ohne sich wirklich über die Konsequenzen im Bezug ihrer dann in den USA gespeicherten personenbezogenen Daten im Klaren zu sein:

- In den USA existiert keine allgemeine und unabhängige Aufsichtsbehörde für den Datenschutz.
- Sämtliche bestehenden Datenschutzregelungen beziehen sich nur auf Bürger der USA und Personen, die sich langfristig in den USA aufhalten, nicht jedoch auf Daten, die aus anderen Staaten in die USA übermittelt werden.
- Im Gegensatz zu Europa gibt es in den USA keinerlei verbindliche Vorgaben über die Speicherfristen gesammelter personenbezogener Daten.
- Es gibt mit der Ausnahme des Freedom of Information Act von 1966 kein Recht auf Auskunft gegenüber Behörden oder Unternehmen, welche personenbezogenen Daten dort gespeichert sind, sowie keinen Rechtsanspruch auf Berichtigung falscher personenbezogenen Daten.
- Die Selbstzertifizierung von US-Unternehmen zu Safe Harbor allein genügt in keinem Fall, um ein den EU-Standards entsprechendes Datenschutzniveau zu erreichen. Die Federal Trade Commission (FTC) schreitet nämlich nur dann ein, wenn ein Unternehmen seine selbst gesetzten Datenschutzrichtlinien nicht einhält.

Die **Safe Harbor** Principles (englisch für „Grundsätze des sicheren Hafens") wurden zwischen 1998 und 2000 im Zusammenhang mit dem Inkrafttreten der europäischen Datenschutzrichtlinie entwickelt um weiterhin einen Datenverkehr zwischen den USA und der EU ermöglichen zu können. Die Datenschutzrichtlinie verbietet es grundsätzlich, personenbezogene Daten aus EG-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EG-Recht vergleichbares Datenschutzniveau verfügen. US-Unternehmen können dem Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die Safe Harbor Principles und die FAQ zu beachten.

Auch wenn die EU im Jahr 2000 anerkannte, dass bei den Unternehmen, die dem Safe-Harbor-System beigetreten sind, ein ausreichender Schutz besteht, stellte 2010 der so genannte Düsseldorfer Kreis (Gremium der Datenschutzbeauftragten des Bundes und der Länder für den nicht-öffentlichen Bereich) fest, dass sich Datenexporteure in Deutschland nicht allein auf die Behauptung einer Safe-Harbor-Zertifizierung von US-amerikanischen Unternehmen verlassen dürfen. Die deutschen Aufsichtsbehörden für den Datenschutz verlangen, dass sich das exportierende Unternehmen vom US-amerikanischen Unternehmen

- die Safe-Harbor-Zertifizierung des US-Unternehmens und
- die Einhaltung der Safe-Harbor-Grundsätze im US-Unternehmen

nachweisen lässt.

Hierzu gehört nach Auffassung der Aufsichtsbehörden, dass deutsche Datenexporteure folgende Mindestprüfungen vornehmen, diese dokumentieren und sie auf Nachfrage den Aufsichtsbehörden nachweisen:

- Datum der Zertifizierung der Datenimporteure: Zertifizierungen, die älter als sieben Jahre sind, sind nicht mehr gültig.
- Einhaltung der Pflicht zur Information der Betroffenen: Gemäß dem Notice-Prinzip in den Safe-Harbor-Grundsätzen hat der Datenimporteur in den USA Privatpersonen darüber zu informieren, zu welchem Zweck personenbezogene Daten erhoben und verwendet werden, wie sich Betroffene mit Nachfragen und Beschwerden an den Datenimporteur wenden können und an welche Dritte die Daten weitergegeben werden.

Aber auch zu Unternehmungen, die ihren Sitz innerhalb der Europäischen Wirtschaftsgemeinschaft (EWG) haben, gab es Eingaben. Hier waren die Petenten oft darüber erstaunt, dass sie wegen der Anwendbarkeit der jeweiligen nationalen Gesetze an die ausländischen Aufsichtsbehörden verwiesen werden mussten.

Illegaler Handel mit E-Mail-Adressen und Spam: Online-Gewinnspiele oft Türöffner für Werbung

Inzwischen sind 97 Prozent des weltweiten E-Mail-Aufkommens Spam. Als Spam werden umgangssprachlich unverlangt zugestellte E-Mails mit werbendem Inhalt bezeichnet. Die bei mir hierzu eingegangenen Eingaben waren oft mit einer angeblichen Einwilligung im Zusammenhang mit Online-Gewinnspielen verbunden. Anhand der protokollierten IP-Adresse in der elektronischen Einwilligung zur Datenerhebung und -verarbeitung wurde regelmäßig festgestellt, dass der unrechtmäßig Beworbene selbst diese Einwilligung nicht abgegeben haben konnte. Sowohl das Telemediengesetz als auch das Bundesdatenschutzgesetz stellen an eine elektronische Einwilligung im Vergleich zu den anderen Einwilligungsverfahren sehr stark abgeschwächte Ansprüche, was die Form und insbesondere die Transparenz gegenüber dem Einwilligenden angeht. Wird die Einwilligung nach § 4a Absatz 1 Satz 3 BDSG in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Diese Ausnahme wird nun offensichtlich dazu genutzt, Einwilligungen durch Dritte zu generieren und dann an interessierte Werbetreibende weiterzuverkaufen.

Eine andere Möglichkeit, wie es zu unverlangten E-Mails mit werbendem Inhalt kommen kann, wobei sowohl der Beworbene als auch der Werbende betrogen werden, ist der Einkauf von günstigen, angeblich über das Opt-In-Verfahren erhobenen E-Mail-Adressen zu Werbezwecken. Im Internet finden sich beispielweise Angebote wie dieses: „12,5 Mio. legale, geprüfte und gepflegte Top-E-Mail-Adressen des Typs Opt-In auf DVD oder zum sofortigen Download Preis: 69,60 Euro". Seriöse Adresshändler verkaufen eine E-Mail-Adresse für etwa einen Cent. In mehreren Fällen führte der Einsatz solcher „Schnäppchen" zu datenschutzrechtlichen Kontrollverfahren gegen die Werbetreibenden. Wer E-Mail-Adressen von Dritten einkauft, darf sich bei deren Nutzung nicht auf die Zusicherung des Verkäufers verlassen, dass für diese Adressen die Einwilligung zum E-Mail-Marketing vorläge, so entschied das OLG Düsseldorf (OLG Düsseldorf, Urt. v. 24.11.2009, I-20 U 137/09). Aufgrund des häufigen Missbrauchs des elektronischen Einwilligungsverfahrens trotz angeblichem Double Opt-in zeigt sich hier Handlungsbedarf.

Opt-in ist ein Verfahren aus dem E-Mail-Marketing, bei dem der Endverbraucher Werbekontaktaufnahmen vorher explizit bestätigen muss. Ein Problem bei einfachem Opt-in im Bereich des E-Mail-Marketings ist, dass beliebige Kontaktdaten zur Anmeldung verwendet werden können, also auch fehlerhafte Daten oder Daten dritter Personen oder Organisationen. Da solche falschen oder missbräuchlichen Einträge immer wieder zu Problemen und Ärger führen, wurde das verbesserte Verfahren „Double Opt-in" entwickelt.

Cloud Computing: Datenschutzskandale vorprogrammiert

Cloud Computing (englisch für: Rechnen in der Wolke) Sammelbegriff für unterschiedlichste IT-Dienstleistungen (z. B. Rechenkapazität, Speicherplatz für Daten oder Computeranwendungen) deren Parameter, jeweils flexibel dem Bedarf des Auftraggebers angepasst, über das Internet zur Verfügung gestellt werden. Weitere Informationen unter www.datenschutzzentrum.de/cloudcomputing

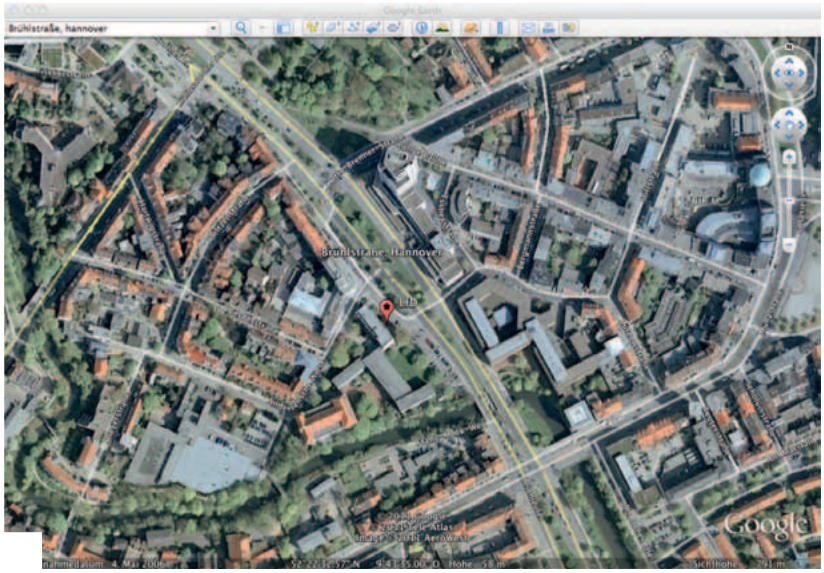
Cloud Computing stellt gegenwärtig neben der Geolokalisierung eine der großen Herausforderungen für den Datenschutz im Internet dar. Sowohl Nutzer als auch Anbieter von Cloud Computing, aber auch Aufsichtsbehörden, sehen sich einer Vielzahl von Problemen gegenübergestellt: Cloud Computing ist tendenziell grenzüberschreitend, es gibt keine technische Notwendigkeit auf territoriale Grenzen Rücksicht zu nehmen. Im Gegensatz dazu ist das Datenschutzrecht an den Ort einer Datenverarbeitung gebunden. Beim Cloud Computing kann sich also sowohl die aufsichtsrechtliche Zuständigkeit wie auch die Verantwortung für eine angemessene und datenschutzkonforme Behandlung von personenbezogenen Daten wortwörtlich in den Wolken verlieren.
Für eine datenschutzrechtliche Bewertung von Cloud-Anwendungen ist daher eine explizite Klärung der Verantwortlichkeiten von zentraler Bedeutung. Die Auslagerung der Datenverarbeitung in andere Staaten hat zur Folge, dass Dritte in diesen Staaten (z.B.: Behörden, Wirtschaftsunternehmen oder Privatpersonen), unter Umständen durch eigene Gesetze legitimiert, Zugriff auf diese Daten bekommen können.
Bei eventuellen Datenschutzverstößen im Zusammenhang mit Cloud Computing außerhalb Deutschlands besteht in der Regel keine Einfluss- oder gar Eingriffsmöglichkeit durch deutsche Aufsichtsbehörden. Gesetzmäßig ist die Datenschutzkontrolle der Aufsichtsbehörden der Bundesländer auf die jeweiligen eigenen Territorien beschränkt. Innerhalb des Bereichs der EU bzw. des EWR könnte zwar theoretisch eine gegenseitige Amtshilfe der Aufsichtsbehörden erfolgen, die aber in der Praxis kaum zur Anwendung kommt.
Tatsache ist: Cloud Computing wird global angeboten und sowohl von deutschen Unternehmen, als auch von Privatleuten und eventuell auch von öffentlichen Stellen genutzt. Dass bisher keine Datenschutzskandale in diesem Zusammenhang bekannt geworden sind, muss jedenfalls kein Anzeichen für ihre Abwesenheit sein.

Geolokalisierung: Wer macht was, wann, wo?

Geolokalisierung auch Geotargeting oder Geolokation genannt, ordnet personenbeziehbare Verkehrsdaten wie IP- oder MAC-Adressen einer geographischen Referenz zu.

Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.

Standortbezogene Telemedien können neben den unbestrittenen Vorteilen für den Nutzer auch Nachteile haben. Kritisch wird es immer dann, wenn personenbezogene Daten gesammelt und daraus Nutzungsprofile erstellt werden können. Neben den Informationen, die bei nicht standortbezogenen Telemedien technisch auch erhoben werden können, bekommen hier Ort und Zeit der Nutzung eine noch stärkere Aussagekraft über die persönlichen Umstände des Nutzers.
Verstärkt werden zur Standortbestimmung nicht nur GPS-Empfänger in mobilen Geräten eingesetzt, sondern auch geographische Ortungsverfahren mittels der MAC-Adressen von Wireless Access Points sowie verschiedenste Lokalisierungsverfahren innerhalb von Mobilfunknetzen. Durch die Verarbeitung der Standortinformationen aus mehreren Lokalisierungsverfahren kann die Standortbestimmung oft bis auf wenige Meter genau erfolgen. Über die Standortbestimmung mittels Verbindungsdaten wie der IP-Adresse des Internetzugangs eines Nutzers von Telemedien lässt sich der Standort in der Regel hingegen nur auf etwa 20 bis 50 km genau schätzen. Mobile Geräte zur Datenverarbeitung wie Smartphones und Netbooks können auf Grund Ihrer geringen



Größe ständig mit sich geführt werden und bieten ständig Zugriff auf Telemedien, was insbesondere bei jüngeren Menschen inzwischen ein nicht mehr wegzudenkender Bestandteil ihres Lebens ist.

Innerhalb des europäischen Projekts „FIDIS – Future of Identity in the Information Society" wurde zwischen 2004 und 2009 in einem Versuch mit vier Teilnehmern deren Bewegungsprofil für den Zeitraum eines Monats mittels GPS erhoben und in einer Datenbank dokumentiert. Bei der Auswertung ließen sich bei den meisten Teilnehmern aus diesen Daten Details des Tagesablaufs, wie z. B. der Arbeitsweg, das dabei genutzte Verkehrsmittel oder die Mittagspause erkennen. Bei allen Teilnehmern waren Rückschlüsse auf den Wohn-, Arbeitsort, sozialen Status, Beruf und Familienstatus möglich. Nur das Geschlecht und Einkaufsverhalten war, vermutlich aufgrund des zu kurzen Beobachtungszeitraums, nicht feststellbar. Auch wenn für diesen Versuch eine relativ große Anzahl von Standortdaten verwendet wurde, so muss man sich vor Augen halten, dass darüber hinaus den Auswertern keinerlei andere Informationen zur Verfügung standen.

Mit Blick auf die Erkenntnisse des FIDIS-Projekts hinterlässt es einen bitteren Nachgeschmack, wenn einer der erfolgreichsten Smartphone-Hersteller in seiner Datenschutzerklärung darlegt, dass sowohl er als auch Dritte in Echtzeit die präzise Standortdaten des Smartphones erheben, nutzen und weitergeben können.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Themen > Internet > Telemedien

Google Street View – die Totalerfassung des öffentlichen Raumes

Die Google Inc. ist ein amerikanischer Telemedien- und Telekommunikationsdienstleister, der nach der Internetsuchmaschine Google benannt wurde. Mit einem Anteil von etwa 80 Prozent aller Suchanfragen im Internet hat Google einen marktbeherrschenden Anteil im internationalen Vergleich der Suchmaschinen.

Google besitzt eine marktbeherrschende Stellung und speichert eine unglaubliche Menge personenbezogener Daten, die miteinander verknüpft werden können.

Das Kerngeschäft von Google ist jedoch der Onlinewerbemarkt, wo die Firma im Jahr 2009 6,5 Milliarden US-Dollar Gewinn erzielte. Fast der gesamte Umsatz wurde mit „interessenbasierter Webung" generiert, ein Verfahren, bei dem von den Nutzern der zahlreichen kostenlosen Google-Dienste Profile erstellt werden, um diesen damit zielgerichtet Werbung zu präsentieren. Wenngleich Google durch die Vielzahl von kostenlosen Diensten wie z. B. You Tube, Google Maps, Google Earth, Google News, Picasa, Gmail (in Deutschland: Google Mail), Google Health, Google Apps und Google Analytics schon quasi omnipräsent im Internet ist, überwacht sie auch das Nutzungsverhalten außerhalb ihrer Dienste über HTTP-Cookies, die im Browser so gesetzt sind, dass eine Rückverfolgung des Benutzers von Webseite zu Webseite möglich ist. Google, das eine marktbeherrschende Stellung besitzt, speichert eine unglaubliche Menge personenbezogener Daten, die miteinander verknüpft werden können. Mit dieser Machtfülle halte ich eine kritische Grenze für überschritten.

Dreidimensionale Vermessung und Daten aus privaten Funknetzwerken

Die rechtliche Bewertung des Abhörens und Aufzeichnens von Daten aus privaten Funknetzwerken wird zur Zeit noch beim zuständigen Hamburgischen Datenschutzbeauftragten geprüft.

Mit dem Dienst Street View begab sich Google zum ersten Mal auch für die Öffentlichkeit wahrnehmbar zum Datensammeln in das „echte Leben". Zwar wurden zuvor bereits durch die Dienste Google Maps und Google Earth mit Hilfe von Luftbildern Einblicke in die Privatsphäre gewährt. Doch die Fahrzeuge mit dem markanten Kameramast und buntem Firmenlogo, die für alle sichtbar durch Stadt und Land fuhren, rückten Street View nun in den Focus des öffentlichen Interesses. Google Street View ist ein Bestandteil des Dienstes Google Maps und des Geoprogramms Google Earth. Hier werden Rundumansichten aus den Einzelbildern mehrerer Kameras erstellt. Die Einzelbilder werden mit speziellen Fahrzeugen aufgenommen. Dabei handelt es sich meist um handelsübliche Personenkraftfahrzeuge, die mit einem Masten ausgestattet sind, an dem in etwa 2,9 Metern Höhe neun Kameras sowie drei Lasermessgeräte zur dreidimensionalen Vermessung befestigt sind. Die Street View-Fahrzeuge verfügen darüber hinaus über eine Empfangsanlage zum Abhören und Aufzeichnen von Sendesignalen von Funknetzwerken. Diese Daten sollen z. B. zur Geolokalisation und Navigation im Dienst Google Latitude dienen. Die rechtliche Bewertung des Abhörens und Aufzeichnens von Daten aus privaten Funknetzwerken wird zur Zeit noch beim zuständigen Hamburgischen Datenschutzbeauftragten geprüft.

Der eigentliche Telemediendienst Street View bietet innerhalb des Dienstes Google Maps und des Geoprogramms Google Earth die Rundumansicht als eine dritte Ansichtsoption neben der reinen Kartenansicht oder der Luftbildansicht. Innerhalb der Rundumansicht kann die Betrachtungsrichtung mit der Maus vertikal und horizontal verändert oder in die vorhergehende oder nachfolgende Rundansicht gewechselt werden. Somit ist es möglich, die Aufnahmestrecke quasi „abzufahren".

Forderungen der Datenschützer umgesetzt

Nicht nur in Deutschland wurde Street View als Eingriff in die Privatsphäre empfunden, auch in Japan, Griechenland, Österreich und der Schweiz musste sich Google wegen Datenschutzproblemen mit den Behörden auseinandersetzen.

Weitere Informationen:
www.datenschutz-hamburg.de

Aufgrund der Zuständigkeit des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit für Google Street View oblag mir für Niedersachsen hauptsächlich die Beratung von Bürgern zu ihren Betroffenenrechten im Rahmen der Vereinbarung zwischen Google und den Aufsichtsbehörden. Auch Gemeinden und Parteien wandten sich mit Beratungs- und Widerspruchswünschen an mich. Allerdings konnten diese als juristische Personen nicht die Regelungen der freiwilligen Vereinbarungen mit Google in Anspruch nehmen, die für den Schutz der Privatsphäre von natürlichen Personen gelten.

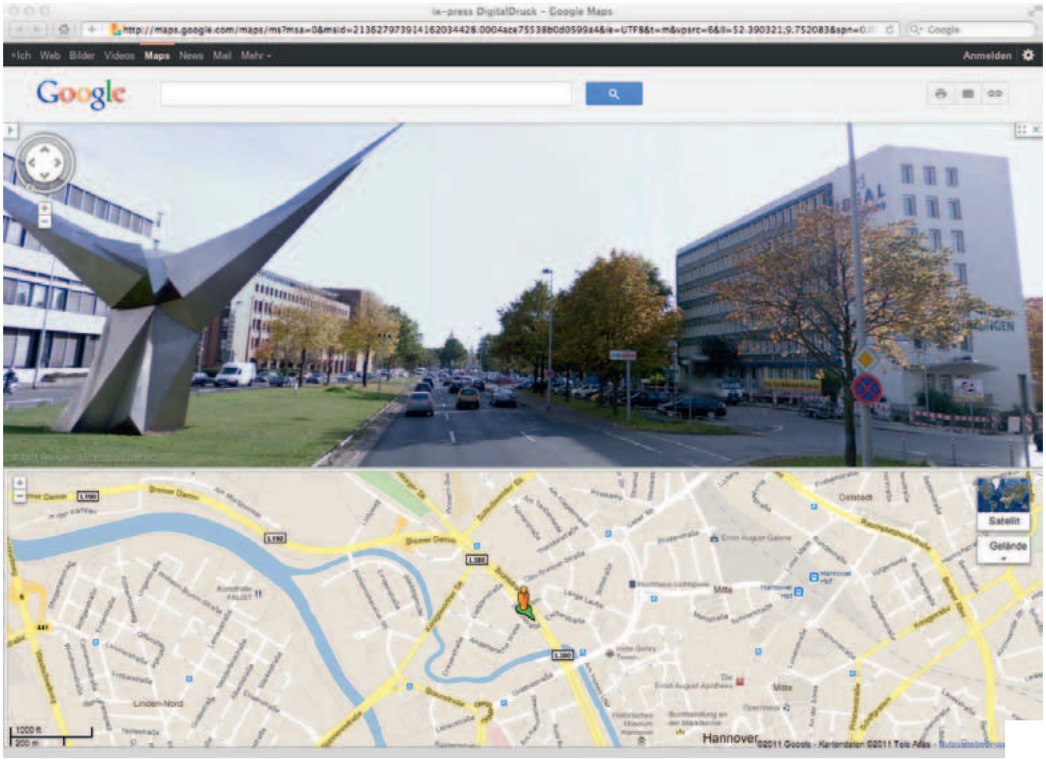
Inzwischen ist Google Street View für 20 Städte Deutschlands im Internet verfügbar. Die vom Düsseldorfer Kreis am 14. November 2008 zum Thema „Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet" beschlossenen Maßnahmen wurden von Google wie zugesichert umgesetzt. Dies betraf unter anderem:

- die geplanten Befahrungen mit einem Hinweis auf die Widerspruchsmöglichkeit rechtzeitig vorher bekanntzugeben,
- eine Technologie zur Verschleierung von Gesichtern und Kfz-Kennzeichen vor der Veröffentlichung derartiger Aufnahmen einzusetzen,
- Widerspruchsmöglichkeiten zur Entfernung bzw. Unkenntlichmachung eines Gebäudes durch einen Bewohner oder Eigentümer vorzuhalten,
- Widersprüche zu Personen, Kennzeichen, Gebäuden und Grundstücken vor Veröffentlichung zu berücksichtigen und die entsprechenden Bilder bereits vor der Veröffentlichung unkenntlich zu machen,
- die Widerspruchsmöglichkeit auch nach der Veröffentlichung vorzuhalten,
- Rohdaten von Personen, Kfz und Gebäudeansichten, die aufgrund eines Widerspruchs zu entfernen sind, zu löschen oder unkenntlich zu machen.

Widersprüche können eingelegt werden im Internet unter https://streetview-deutschland.appspot.com/submission oder schriftlich bei der Google Germany GmbH, betr.: Street View, ABC-Straße 19, 20354 Hamburg.

Verpixeln und Entpixeln

Kurios ist in diesem Zusammenhang der „Widerspruch zum Widerspruch", verkündet von einem Blogger und Werbetexter, der Dritte in die Lage versetzen soll, Fassaden eines Bauwerks im Google-Dienst wiederherzustellen, selbst wenn Bewohner oder Eigentümer dies nicht wünschen. Wenngleich eine deutsche Computer-Fachzeitschrift



Quelle:
http://maps.google.com

unter dem Titel: „So entpixeln Sie Häuser bei Street View!“ eine Video-Anleitung veröffentlicht hat, so scheint diese Bewegung keinen nennenswerten Zulauf erhalten zu haben. Eine systematische Umgehung der Widersprüche in Niedersachsen ist jedenfalls nicht bekannt.

Es ist nicht zulässig, mit Diensten wie Panoramio (Google) oder Flickr (Yahoo) die Unkenntlichmachung von Häuseransichten in Street View zu umgehen

Nach Ansicht der Datenschutzaufsichtsbehörden ist es nicht zulässig, mit Diensten wie Panoramio (Google) oder Flickr (Yahoo) die Unkenntlichmachung von Häuseransichten in Street View zu umgehen. Google muss sicherstellen, dass verpixelte Häuser nicht als Foto gezeigt werden können.

Selbstverpflichtung der Wirtschaft reicht nicht aus

Die Datenschutzbeauftragten von Bund und Ländern bestehen auf einer strengen gesetzlichen Regulierung der Online-Veröffentlichung von personenbezogenen Daten und Geoinformationen und damit auch auf einer gesetzlichen Regelung des Widerspruchsrechts von Betroffenen gegen die Veröffentlichung ihrer Daten im Internet. Leider wurden die Vorschläge des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) zur Regulierung personenbezogener Internetdatenveröffentlichungen (https://www.datenschutzzentrum.de/internet/20101027-gesetzentwurf-internetveroeffentlichungen.html) aus dem Oktober 2010 nicht von der Politik aufgegriffen. Stattdessen stellte der Bundesinnenminister am 1. Dezember den Inhalt eines eigenen Gesetzentwurfs vor, der den Schutz vor besonders schweren Persönlichkeitsrechtsverletzungen im Internet verbessern soll.

Die Bundesregierung hatte sich nach einem Geodaten-Gipfelgespräch vor allem für eine Selbstverpflichtung der Wirtschaft im Zusammenhang mit Telemedien wie Google

Street View ausgesprochen. Nach Ansicht der Aufsichtsbehörden greift dieser Lösungsansatz aber deutlich zu kurz, denn eine Selbstverpflichtung kann gesetzliche Regelungen nicht ersetzen. Weder sind die Unternehmen, die der Selbstverpflichtungserklärung nicht beitreten, künftig verpflichtet, die Vorgaben einzuhalten, noch lassen sich Verstöße gegen den Kodex durch eine selbständige Datenaufsicht durchsetzen und sanktionieren.
Der Vorstand des Verbraucherzentrale-Bundesverbands (vzbv) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), der nachdrücklich eine umfassende Modernisierung des Datenschutzes forderte, legten deshalb einen alternativen „Fünf-Punkte-Plan“ vor:

Fünf-Punkte-Plan

1. Gesetzlichen Rahmen verbessern
Die wesentlichen Verbraucher- und Datenschutzrechte gehören ins Gesetz. Dazu gehört ein verbrieftes Widerspruchsrecht der Betroffenen gegen die Veröffentlichung ihrer Daten im Internet sowie das Verbot mit Erlaubnisvorbehalt der Zusammenführung und Verknüpfung personenbezogener Daten.

2. Freiwillige Selbstverpflichtungen verbindlicher machen
Freiwillige Selbstverpflichtungen sind grundsätzlich zu begrüßen. Sie müssen aber mit Kontrollen und Sanktionen bei Nichteinhaltung begleitet werden. Eine Selbstverpflichtung ersetzt kein verbrieftes, einklagbares Recht auf Widerspruch.

3. Verbraucher- und Datenschutz international durchsetzen
Safe Harbour, das Abkommen zwischen der Europäischen Union und den USA über die Einhaltung des Datenschutzes, muss verbessert und effektiv durchgesetzt werden. Internetdienste, die unter dieses Abkommen fallen, müssen sich an europäisches beziehungsweise nationales Recht halten und dies auch gegenüber den Nutzern kenntlich machen.

Zum Thema Safe Harbour siehe auch Seite 52

4. Technologischen Datenschutz stärken
Bei der Entwicklung neuer Technologien müssen die Erfordernisse des Datenschutzes frühzeitig berücksichtigt werden („privacy by design“). Zudem sollten die Voreinstellungen von sozialen Netzwerken oder bei Browsern standardmäßig ein hohes Datenschutz- und Verbraucherschutzniveau aufweisen („privacy by default“).

5. Datenerhebung und -verarbeitung transparent gestalten
Informationen über eingesetzte Techniken der Datenerhebung und -verarbeitung müssen situativ angemessen, verständlich und leicht abrufbar sein. Einwilligungen in die Erhebung und Verarbeitung von Daten sollten zeitlich begrenzt sein. Eine aktive, informierte Einwilligung ist verbindlich umzusetzen.

Datenschutzbeauftragte bestellen? Viele Betriebe unsicher

Die aufgedeckten Datenpannen und Datenmissbräuche der letzten Jahre lassen die Bedeutung des professionellen Umganges mit dem Datenschutz und auch die damit verbundene Stellung des qualifizierten und unabhängigen Datenschutzbeauftragten in den einzelnen Unternehmen immer mehr in den Vordergrund rücken.

Anfragen der täglichen Praxis spiegeln wider, dass in vielen Betrieben Unsicherheit herrscht, ob und wie die Bestellung eines betrieblichen Datenschutzbeauftragten umgesetzt werden soll. Des weiteren häufen sich Fragen zur Interessenkollision im Rahmen der Zuverlässigkeit und zur Fachkunde der betrieblichen und externen Datenschutzbeauftragten. Nicht-öffentliche Stellen, die personenbezogene Daten gem. § 1 Abs. 2 Nr. 3 BDSG automatisiert verarbeiten, sind verpflichtet, dem Landesbeauftragten für den Datenschutz Niedersachsen als zuständige Datenschutzaufsichtsbehörde Verfahrensverzeichnisse gem. § 4 d Abs. 1 i. V. m. § 4 e BDSG zu melden. Die Meldepflicht entfällt, wenn gem. § 4 f BDSG ein Beauftragter für den Datenschutz bestellt wird. Mein Webangebot www.lfd.niedersachsen.de bietet unter Themen/Datenschutzbeauftragte/betriebliche Datenschutzbeauftragte Interessierten einen kurzen Überblick zur Rechtslage.

Schwerpunktkontrolle Zeitarbeitsfirmen

Anlässlich der Fragebogenaktion des Hamburgischen Datenschutzbeauftragten bei den Unternehmen der Hansestadt zum Vorhandensein betrieblicher Datenschutzbeauftragter habe ich auch in Niedersachsen eine ähnliche anlassunabhängige Kontrolle bei Zeitarbeitsfirmen durchgeführt. Bei Unternehmen, die bisher keine Meldung gemäß § 4 d BDSG zum Melderegister abgegeben hatten, wurde nach Vorhandensein eines betrieblichen Datenschutzbeauftragten gefragt und wie bei jeder Prüfung auf die Auskunftspflicht sowie das Auskunftsverweigerungsrecht (§ 38 BDSG) hingewiesen.
Um eine Auswahl aus allen niedersächsischen Zeitarbeitsfirmen treffen zu können, forderte ich von der Regionaldirektion Niedersachsen-Bremen der Bundesagentur für Arbeit in Hannover eine Auflistung aller Inhaber einer Erlaubnis von Betrieben an, die ausschließlich oder überwiegend Arbeitnehmerüberlassung betreiben.

Nicht-öffentliche Stellen sind gem. § 2 Abs. 4 BDSG natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts.

47 Betriebe ausgewählt

Nach dem Zufallsprinzip wurden 47 Betriebe für die Kontrolle ausgewählt. Als Anlage zu dem Anschreiben erhielten die Firmen neben dem Haupt- und Anlageblatt zur Anmeldung ein Merkblatt zur Meldepflicht. Das ebenfalls beigelegte

Info-Fragenblatt zum betrieblichen Datenschutzbeauftragten beinhaltete unter anderem die Fragen nach

- der betrieblichen Stellung,
- der Aufgabenwahrnehmung bei nebenamtlicher Tätigkeit,
- der Kurzbeschreibung des beruflichen Werdegangs,
- der datenschutzrechtlichen Vorkenntnisse,
- der bereits abgeschlossenen Maßnahmen,
- der geplanten Fortbildung und
- den wahrzunehmenden Aufgaben im Betrieb.

Durch die Beantwortung der Fragen und anhand der vorgelegten Zertifikate für entsprechende Fachausbildungslehrgänge erhielt ich neben den Bestellungsurkunden einen Einblick in den Ausbildungsstand der einzelnen betrieblichen und externen Datenschutzbeauftragten.
Bislang gibt es keine rechtlich spezifizierten Berufsanforderungen. In der gesetzlichen Vorgabe des § 4 f Abs. 2 BDSG werden die Anforderungen an den Datenschutzbeauftragten lediglich mit „Fachkunde“ und „Zuverlässigkeit“ beschrieben. Ein berufliches Leitbild des Datenschutzbeauftragten wurde als Maßstab von der Mitgliederversammlung des Berufsverbands der Datenschutzbeauftragten Deutschlands e. V. (BvD) im September 2009 verabschiedet und im April 2010 angepasst. Entsprechende Aus- und Fortbildungsveranstaltungen für betriebliche Datenschutzbeauftragte werden von verschiedenen Institutionen angeboten. Auf Anfrage – jedoch ohne Bewertung durch die Aufsichtsbehörde – werden diese Bildungsangebote an Interessierte weitergegeben.

Personenbezogene Daten
sind gem. § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Automatisierte Verarbeitung
ist gem. § 3 Abs. 2 BDSG die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.

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

Ergebnis

Die Gesamtauswertung der Kontrolle ergab, dass von den 47 überprüften Betrieben 38 keiner Meldepflicht unterlagen, da mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten nur ein bis drei Mitarbeiter beschäftigt sind und die Daten nur für eigene Zwecke erhoben oder nicht automatisiert verarbeitet werden. Einen Nachweis für die Bestellung eines Datenschutzbeauftragten erbrachten acht Betriebe. Ein Betrieb unterlag der Meldepflicht zum Verfahrensverzeichnis.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Themen > Datenschutzbeauftragte > betriebliche Datenschutzbeauftragte

Datensünder bestrafen – Bußgeldverfahren im Datenschutzrecht

Datensünder müssen seit einiger Zeit verstärkt damit rechnen, dass ihr Zuwiderhandeln gegen Datenschutzvorschriften neben weiteren denkbaren aufsichtsbehördlichen Maßnahmen auch mit der Verhängung eines Bußgeldes geahndet wird.

Die datenschutzrechtlichen Aufsichtsbehörden in den Bundesländern sind, sofern nicht-öffentliche Stellen betroffen sind, auch Bußgeldbehörden. Mit der im Jahr 2009 begonnenen Personalverstärkung des für den nicht-öffentlichen Bereich zuständigen Teils meiner Behörde ist dieser Aufgabenbereich deutlich vergrößert worden, und es werden vermehrt Bußgeldverfahren durchgeführt. Zwar liegt der Schwerpunkt meiner Tätigkeit nach wie vor in der Beratung der für Datenverarbeitung verantwortlichen Stellen, und es wird zunächst ein kooperativer Ansatz verfolgt. Doch der leider weiterhin verbreitete nachlässige Umgang mit Datenschutzvorschriften findet seine Resonanz auch in der Anwendung der gesetzlich zur Ahndung von Ordnungswidrigkeiten aufgestellten Bußgeldvorschriften. Insbesondere aus generalpräventiven Gründen ist eine nachdrücklichere Ahndung von Datenschutzverstößen angezeigt, die auch formeller Art sein können wie die Auskunftspflichtverletzung oder die Nichtbestellung eines betrieblichen Datenschutzbeauftragten.

Ordnungswidrigkeitentatbestände

Das Datenschutzrecht beinhaltet zahlreiche Ordnungswidrigkeitentatbestände. In § 43 Bundesdatenschutzgesetz (BDSG) sind die Wichtigsten aufgeführt; als Beispiele seien genannt die unbefugte Datenverarbeitung, der unbefugte Datenabruf, die Verletzung der Auskunftspflicht gegenüber dem Betroffenen bzw. gegenüber der Aufsichtsbehörde, das Unterlassen der Bestellung eines betrieblichen Datenschutzbeauftragten oder die ungenügende Erteilung eines Auftrags im Rahmen einer Auftragsdatenverarbeitung. Mit Novellierung des BDSG sind in diesem Bereich weitere Tatbestände hinzugekommen, wie Werbung trotz Vorliegens eines Werbewiderspruches oder das Unterlassen einer Meldung an die Aufsichtsbehörde beim Auftreten eines massiven Datenlecks. Auch das Telemediengesetz (TMG) für den Bereich des Datenschutzes im Internet enthält Ordnungswidrigkeitentatbestände in § 16, z. B. bei unbefugter Datenerhebung durch Internetdienste, bei unbefugtem Erstellen eines Profils der Internetnutzer und bei Fehlen einer Datenschutzerklärung auf einer Internetseite.
Die Höhe des Bußgeldes kann zunächst bis zu 300.000 Euro betragen; reicht dieser Betrag zur Ahndung im Einzelfall nicht aus, kann er jedoch auch überschritten werden. Die Zumessung des Bußgeldes richtet sich danach, ob es sich um einen formellen oder materiellen Verstoß handelt, wie groß das Ausmaß der Verletzung ist (Anzahl der Betroffenen, mögliche Folgen für die Betroffenen), ob es sich um einen Einzelfall oder eine Wiederholungstat handelt und ob sich die beschuldigte Stelle einsichtig zeigt. Gegen Unternehmen können so genannte selbständige Ordnungswidrigkeitenverfahren durchgeführt werden, wenn Datenschutzvorschriften durch ihre verantwortlich handelnden Vertreter nicht beachtet werden. Die Verantwortlichkeit für die Beachtung der Datenschutzvorschriften trifft in der Regel den Inhaber bzw.

Repräsentanten des Unternehmens (z. B. Meldepflicht, Auskunftspflicht, Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten).

35 Ordnungswidrigkeitenverfahren eingeleitet

In den Jahren 2009 und 2010 habe ich insgesamt 35 Ordnungswidrigkeitenverfahren eingeleitet. Eine Analyse nach Häufigkeit der Verfolgung einzelner Ordnungswidrigkeitentatbestände zeigt, dass eine ungenügende, verspätete oder vollständig unterlassene Auskunftserteilung an mich bzw. an den Betroffenen der am häufigsten von mir im Bußgeldverfahren geahndete Tatbestand war. Hierbei reagieren die Betroffenen nicht genügend auf die Anforderungen durch mich als Aufsichtsbehörde oder auch durch den Betroffenen selbst zur Erteilung von Auskunft über die Datenverarbeitung in einem Unternehmen, obwohl nach dem BDSG eine eindeutige Pflicht zur Auskunftserteilung besteht. Diese Verstöße werden nun deutlich strenger verfolgt. Die Auskunftsaufforderung ist der erste Schritt in einem aufsichtsbehördlichen Kontrollverfahren, eine fehlende Mitwirkung bereits in diesem frühen Stadium zeigt daher bereits oft eine Missachtung des Datenschutzrechts. Gravierende Datenschutzverstöße können so auch oft erst verspätet entdeckt werden. Diese Verstöße wurden von mir mit einem Bußgeld in einer Höhe von 250 bis 800 Euro geahndet, je nach Größe bzw. wirtschaftlicher Aufstellung der betroffenen Stelle.

Daten im Abfall

Leider kommt es auch immer noch zu einer illegalen Entsorgung von personenbezogenen Daten. Hierzu sind mehrere Fälle in 2009 und 2010 bearbeitet worden. Es handelte sich dabei meist um nicht mehr benötigte Bewerbungsunterlagen, die nach Abschluss einer Bewerberrunde schlicht im Müll gelandet waren. Doch sogar besonders sensible Gesundheitsdaten in Form von Patientenakten wurden bereits in einem Altpapiercontainer aufgefunden. Hier ist eine oft erschreckende Gedankenlosigkeit der mit Daten arbeitenden Stellen zu erkennen. Es sollte jedoch selbstverständlich sein, dass personenbezogene Daten, die mit einem gewissen Vertrauen übergeben wurden, nicht einfach mit anderem Müll zu entsorgen sind. Dieses Verhalten stellt rechtlich eine vorsätzliche unbefugte Datenverarbeitung dar. Aufgrund der in diesen Fällen großen Anzahl der konkret Betroffenen sowie aufgrund der großen möglichen Schäden für diese habe ich in einem Einzelfall ein Bußgeld in Höhe von mehreren tausend Euro verhängt.

Unbefugte Abfrage bei Schufa & Co.

Auch die unbefugte Abfrage von Informationen über Dritte bei Wirtschaftsauskunfteien war Gegenstand mehrerer Ordnungswidrigkeitenverfahren. Hierbei fehlte es jeweils an dem anzugebenden berechtigten Interesse an einer Abfrage, oder es wurden bewusst falsche Angaben gemacht. Bei diesem Datenschutzverstoß wird die Möglichkeit zur selbständigen Abfrage

ohne genauere Überprüfung der Angaben durch die Auskunftei bewusst missbraucht. Gerade in diesem Bereich ist vielen nicht bewusst, dass auch die kurze Abfrage zu einer Person bei einer Auskunftei bereits dort gespeichert wird und negative Folgen für die betroffene Person haben kann. Daher wurde auch in diesen konkreten Fällen ein empfindliches Bußgeld von jeweils mehreren tausend Euro verhängt.
Zu diesem Bereich gehört auch die unbefugte Abfrage von Daten aus dem elektronisch geführten Grundbuch. Konkret hatte eine Bank eine solche Abfrage mit Hilfe des vorab eingeräumten generellen Zugangs zum elektronisch geführten Grundbuch getätigt, ohne jedoch tatsächlich über ein berechtigendes Interesse zu verfügen. Auch ein solches missbräuchliches Ausnutzen einer einmal erteilten Befugnis stellt ein bußgeldwürdiges Verhalten dar. Im konkreten Fall hatte der Vertreter dieser Bank ein Bußgeld in Höhe von 3.000 Euro zu zahlen.

Internet

Die in den Jahren 2009 und 2010 verfolgten Ordnungswidrigkeitentatbestände aus dem Telemedienbereich betreffen vor allem das unbefugte Speichern von Daten wie z. B. von IP-Adressen (die als personenbeziehbare Daten anzusehen sind) oder das Unterlassen einer Löschung bzw. Sperrung von nicht mehr erforderlichen Daten der Nutzer von Internetseiten.

Beratung statt Bußgeld

In vielen Fällen nehmen die Betroffenen dahingehend Stellung, dass eine Unkenntnis der relevanten datenschutzrechtlichen Vorschriften bestanden habe. Auch wenn eine Kenntnis der einschlägigen Rechtsvorschriften bei den Daten verarbeitenden Stellen vorauszusetzen ist, zeigt dies erneut, wie wesentlich der von mir mit meiner Tätigkeit primär verfolgte Zweck der Beratung ist. In einigen Fällen übe ich das mir für die Durchführung von Ordnungswidrigkeitenverfahren gesetzlich zugestandene Ermessen folglich in Richtung einer Beratung für die Zukunft aus und sehe von der Verhängung eines Bußgeldes ab.
Wird ein Bußgeldbescheid mit einem Einspruch angegriffen, wird das Verfahren an die Staatsanwaltschaft Hannover weitergegeben. Die inzwischen gemachten Erfahrungen mit den hiesigen für die Bearbeitung von Ordnungswidrigkeitenverfahren zuständigen Richtern zeigen, dass meine Einschätzungen zu Datenschutzverstößen geteilt werden.

Weitere Informationen:

www.gesetze-im-internet.de/owig
www.gesetze-im-internet.de/bdsg
www.gesetze-im-internet.de/tmg

3

Technisch-organisatorischer Datenschutz

Schlechte Produkte, Dataleaks, Malware und Bots: Fehlendes Management öffnet Tür und Tor

Datenschutz funktioniert in der Praxis nur, wenn Schutzvorschriften wie Gebote und Verbote und datenschutzrechtliche Grundsätze eingehalten werden. Aber damit ist nur der juristische Teil betrachtet. Immer mehr Bedeutung bekommt auch die Frage, ob die Entwicklung von Lösungen und Maßnahmen zur IT-Sicherheit bei Hard- und Software hinreichend wirksam umgesetzt wird. Dabei wird das zu betrachtende Umfeld immer komplexer. Betroffen sind IT-Verfahren, Standardsoftware, Internetanwendungen, Buchungssysteme, das Internet und seine Komponenten, leitungsgebundene Netze, Funknetze sowie Hardware im Rechenzentrum, am Arbeitsplatz und in Form von mobilen Geräten wie Smartphones, Tablet-PC, Laptops oder Navigationsgeräten.

Während in professionellen Umgebungen wie Rechenzentren oder großen Netzen ein systematisches Informationssicherheitsmanagement als Standard zu betrachten ist, fehlt es in der Praxis allzu oft an wirksamen und lückenlosen Maßnahmen zur Absicherung der zahllosen immer mehr vernetzten Einzelkomponenten. Software kommt auf den Markt, die noch unausgereift ist, Sicherheitslücken werden spät oder gar nicht entdeckt. Angreifer suchen und finden diese Lücken und entwickeln eine Vielzahl von so genannten Exploits, also Schadprogramme oder Skripts, die diese Sicherheitslücken für programmtechnische Möglichkeiten zur Manipulation von Systemen und Daten oder zum Datendiebstahl ausnutzen. Malware wie trojanische Pferde präparieren Rechner dafür, sich selbst – unbemerkt vom Besitzer – aus dem Netz von Servern eine Software herunterzuladen, die als Steuerungssoftware den Befehlsempfang vom Täterserver ermöglicht. So entstehen Botnetze mit tausenden infizierten „Zombierechnern", ohne dass deren Besitzer vom Eigenleben ihres Rechners etwas wissen. Die so infizierten Systeme lassen sich sogar im Verbund für rechenintensive Massenarbeiten für kriminelle Ziele missbrauchen, etwa zur weiteren Verbreitung trojanischer Pferde, zum Spamversand oder für das Versenden von Phishing-Mails.

Botnetze mit tausenden unbemerkt infizierten „Zombierechnern" lassen sich für kriminelle Ziele missbrauchen.

Angreifer kaufen sich am Schwarzmarkt fertige Baukastensysteme, die diese Exploits und eine Menge „Komfort" beinhalten und bereits fertige Angriffsszenarien bieten – gewissermaßen Werkzeugkoffer für den Beutezug. Es gilt also, diesen Angriffen auf die Systeme und die Daten präventiv und systematisch etwas entgegenzusetzen. Unwissenheit oder Ignoranz bei der Systemverwaltung käme dem Offenstehenlassen der Haustür gleich. Zahl-

reichen Studien zufolge – nicht zuletzt laut Lageberichten des BSI – ist die Sicherheitslage im IT-Bereich alles andere als befriedigend. Das BKA spricht in seiner Polizeilichen Kriminalstatistik 2010[1] von 84.377 Fällen der Computerkriminalität, was eine Steigerung gegenüber 2009 von 12,6 Prozent entspricht. Darunter fällt auch das Ausspähen und Abfangen von Daten mit einer Steigerungsrate von 32,2 Prozent. Eine Umfrage des amerikanischen Softwareherstellers Symantec unter 2.100 Betrieben hatte 2010 ergeben, dass drei Viertel aller Firmen weltweit im Jahr 2009 Opfer von Cyber-Attacken waren.

IT-Sicherheitspaket nur in jedem zehnten Unternehmen

Laut dem IT-Sicherheitsverband TeleTrusT Deutschland e. V.[2] hat das von diesem mit betreute „Netzwerk Elektronischer Geschäftsverkehr" (NEG) 2010 eine Untersuchung durchgeführt, bei der Mängel bei klein- und mittelständischen Unternehmen hinsichtlich der IT-Sicherheit festgestellt wurden. In vielen Fällen fände die IT-Sicherheit keine ausreichende Beachtung, und nur jedes zehnte Unternehmen verfüge über ein IT-Sicherheitspaket. Knapp zwei Drittel der befragten kleinen und mittelständischen Unternehmen hätten bislang überhaupt keine Maßnahmen umgesetzt. Bedenklich ist meines Erachtens vor allem, dass sich nach diesen Studien nur eine knappe Mehrheit von 56 Prozent darüber bewusst sein soll, dass sich die Unternehmen ohne entsprechenden Schutz, wie z. B. Verschlüsselung, angreifbar machen. Sogar 44 Prozent der Befragten beschäftigten sich überhaupt nicht mit dem Thema „IT-Sicherheit", und ein weiteres Viertel habe sich zwar bereits mit dem Thema auseinandergesetzt, bislang jedoch noch keine ausreichenden Schutzvorkehrungen getroffen.

Leider kann ich aus meinen eigenen Feststellungen in der datenschutzrechtlichen Beratungs- und Prüfpraxis diesen ernüchternden Zahlen nicht widersprechen. Je kleiner ein Betrieb ist, desto weniger Personalkapazitäten werden in die Professionalisierung der IT-Sicherheit und des technischen Datenschutzes investiert. Auch im öffentlichen Bereich gilt grundsätzlich diese Erkenntnis. Je größer ein Unternehmen, eine Organisation, eine Behörde ist, desto eher ist nach meinen Erkenntnissen zunächst einmal die Chance gegeben, dass es eine Kompetenzstelle gibt, die sich systematisch, standardisiert und nach dem Stand der Technik mit IT-Sicherheit befasst und notwendige Vorkehrungen durchsetzen kann. Eine Entwarnung allerdings, dass in allen großen Betrieben und Behördenbereichen alles in bester Ordnung sei, kann dagegen nicht gegeben werden. Je größer und komplexer die IT-Landschaft wird, desto anspruchsvoller werden auch die Anforderungen an die Sicherheit und an das Fachpersonal.

Je kleiner ein Betrieb ist, desto weniger Personalkapazitäten werden in die Professionalisierung der IT-Sicherheit und des technischen Datenschutzes investiert.

Am Beispiel von Servern, die in großer Stückzahl in einem Rechenzentrum stehen, ist leicht vorstellbar, dass der administrative Aufwand bei einheitlicher Ausstattung für das Ausrollen eines Sicherheitsupdates mit standardisiertem Verfahren im Verhältnis erheblich geringer ist als in kleinen Organisationseinheiten. Wird in diesem Großbereich ein sicherheitskritisches Update dagegen vergessen oder aus betriebswirtschaftlichen Gründen unterlassen, kann die entstehende Sicherheitslücke zu einem Totalausfall der Verfügbarkeit oder zu einem fatalen Angriff auf Millionen Kundendatensätze mit dem Verlust der Integrität und Vertraulichkeit der Daten führen. Daher kommt es bei allen Komponenten der Hard- und Software sowie im

1 Bundesinnenministerium: „Polizeiliche Kriminalstatistik 2010" (http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2011/PKS2010.pdf?__blob=publicationFile)

2 Teletrust Pressemitteilung vom 08.12.2010 http://www.teletrust.de/uploads/media/PM-2010-12-08-TeleTrusT-IT-Sicherheit.pdf

organisatorischen Umfeld auf die Vollständigkeit der Schutzbedarfs-, Risiko- und Sicherheitsanalysen sowie die angemessenen Schutzmaßnahmen an.

Mehr Datenschutz durch „privacy by design“

Wie ich in meinem letzten Tätigkeitsbericht bereits ausgeführt hatte, stellt der überproportionale Anstieg bei der Verbreitung mobiler Endgeräte die Arbeitsprozesse und das persönliche Verhalten der Nutzer völlig um. Immer mehr Daten – auch personenbezogene – werden von den Menschen in der Tasche herumgetragen, über Netze repliziert, mit anderen Endgeräten synchronisiert und in das Internet bei Cloud-Diensteprovidern gespeichert. Diese Veränderungen machen Smartphones als digitale Alleskönner besonders attraktiv für Angriffsversuche durch Hacker mit kriminellen Absichten. Manche Kontrolle geht dem Benutzer dabei verloren, weil nicht alle Komponenten, Sicherheitslücken und notwendige wirksame Sicherheitsmaßnahmen bekannt sind. Daher gilt:

- Hersteller, Systementwickler, Diensteanbieter und IT-Verfahrensverantwortliche bleiben aufgefordert, dem Grundsatz „privacy by design“ zu folgen und bei der Entwicklung von IT-Anwendungen, Hard- und Software sowie Standardverfahren den technischen Datenschutz konzeptionell mitzudenken und gleich als Voreinstellung zu implementieren („privacy by default“).
- Der Handel und die Beratungsbranchen bleiben aufgefordert, kompetente Beratung bei der Auswahl von datenschutzgerechten Alternativen walten zu lassen.
- Rechenzentren, Diensteanbieter, Provider und IT-Verantwortliche bleiben aufgefordert, ein IT-Sicherheitsmanagement und ein Datenschutzmanagement aufzubauen und technisch-organisatorischen Datenschutz als lebenserhaltende Maßnahmen zu begreifen.
- Nutzer müssen weiter an der eigenen Medien- und IT-Kompetenz arbeiten. Sie bleiben aufgefordert, den Selbstdatenschutz bei der Nutzung von Diensten, Netzen, Computern und Smartphones mehr Beachtung zu schenken. Wer im Straßenverkehr ein Kraftfahrzeug führt, akzeptiert Selbstsicherungen wie das Anlegen des Gurtes, das Einhalten von HU-Terminen und die rechtzeitige Fahrzeugwartung, aber auch Gesetze mit Schranken, Verboten und Geboten zum Schutz aller. Dasselbe sollte im eigenen Interesse und im Interesse eines hohen Sicherheitsniveaus für die Daten auch im Bereich der IT gelten.

Datenlecks durch Designfehler: Dringender Gesetzgebungsbedarf

Immer öfter beherrschen Sicherheitsvorfälle die Schlagzeilen: „Adressdaten illegal verkauft", „Kundendatensätze gestohlen", „Webseiten geknackt", „Server gehackt" – so oder ähnlich lauten die Meldungen in den Medien. Inzwischen wird mitunter mehrfach je Woche ein neuer Datenskandal öffentlich. Neben der juristischen Frage der Verletzung von Datenschutzbestimmungen, die stets zu prüfen ist, ist in den meisten Fällen auch die Frage zu stellen, ob in dem Vorfall die technischen und organisatorischen Schutzmaßnahmen rund um die betroffenen Systeme der Informationstechnik ausreichend geplant und implementiert waren. Außerdem sind die Organisationsprozesse und das gesamte IT-Sicherheitsmanagement zu hinterfragen. Diese systematischen Aspekte des technisch-organisatorischen Datenschutzes sind elementarer Bestandteil zur Gewährleistung der Datenschutzziele.

Die Zahl der tatsächlichen Angriffsflächen ist bei heutigen Informationssystemen aufgrund ihrer Anzahl und wegen ihrer Komplexität, ihrer Verflechtungen untereinander und ihrer standardmäßig vorhandenen Internetverbindungen erheblich gestiegen. Ein einziger Designfehler eines Mikrochips oder ein Implementierungsfehler im Design einer Standardsoftware, etwa des Betriebssystems, eines Datenbankmanagementsystems, einer Anwendungssoftware oder einer Smartphone-App, genügt, um Vertraulichkeit und Integrität der Daten von tausenden oder gar Millionen Anwendern im gewerblichen, behördlichen oder privaten Bereich zu gefährden.
Wenn Designfehler zu systematischen Angriffstoren gegen IT-Systeme und damit gegen die Integrität und Vertraulichkeit von Systemen und Daten führen können, muss demzufolge einer der Lösungsansätze lauten, Datenschutz im Designstadium von IT-Verfahren und besser noch in einzelnen IT-Komponenten der Hard- und Software zu etablieren. Dieser Ansatz wird mit „privacy by design" bezeichnet. Die Praxis zeigt, dass dies oft von Herstellern und Entwicklern versäumt wird, weil betriebswirtschaftliche Interessen höher gestellt werden. Es gibt aber zusätzlich auch gesetzliche Definitionsprobleme und Schwierigkeiten in der operationalen Umsetzung des Ansatzes von „privacy by design". Aus diesem Grund haben sich die Datenschutzbeauftragten des Bundes und der Länder der Problematik besonders angenommen.

„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

Technisch-organisatorische Maßnahmen oft zu schwach

Das System der Schutzmaßnahmen im öffentlichen Bereich ist derzeit im § 7 NDSG durch so genannte Kontrollziele definiert. Es sind dies Zugangskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, Zugriffskontrolle, Übermittlungskontrolle, Eingabekontrolle, Verfügbarkeitskontrolle, Auftragskontrolle, Transportkontrolle und Organisationskontrolle. Die Entsprechung finden diese Kontrollziele im nicht-öffentlichen Bereich im § 9 BDSG und seiner dazu ergangenen Anlage. Diese Ziele fokussieren die Maßnahmen auf die Art des Umgangs mit Daten, ausgehend von einem monolithischen System, dessen Systemgrenze klar definiert ist und die es zu schützen gilt. Entstanden sind diese Regelungen in den 1970er-Jahren. Die gesetzliche Regelung, dass der Aufwand für die Maßnahmen unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen muss, wird von Verfahrens-

verantwortlichen nach meiner Erfahrung praktisch oft als Begründung dafür strapaziert, einfachere Schutzmaßnahmen aufwändigeren und damit kostenintensiveren Maßnahmen vorzuziehen. Damit gewinnen wirtschaftliche Beweggründe gegenüber sicherheitsorientierten zu oft die Oberhand. Dass sich die Maßnahmen nach dem Stand der Technik richten müssen, bedeutet jedoch auch, sie regelmäßig fortzuschreiben. Tendenziell müssten sie aufgrund der oben beschriebenen technischen Verdichtung der Systeme, der Zunahme der Komplexität und der Allgegenwärtigkeit von Computern also eher verschärft und ergänzt als abgeschwächt werden.

Schutzbedarf richtig erkennen, Risiken nicht unterschätzen!

In der Praxis werden häufig sowohl der Schutzbedarf der betroffenen Daten und Informationen, als auch das Risiko des Schadeneintritts und die Schadenshöhe unterschätzt. Vor allem wird oft unterschätzt, wie viele Sicherheitslecks existieren. Auch wenn diese dem Nutzer und selbst IT-Betrieben oft noch unbekannt sind, werden sie in der Hackerszene schon längst buchstäblich gehandelt. Mit krimineller Energie lassen sich diese durch Schadprogramme (so genannte Exploits) nutzen. Dem Ausbau der IT-Sicherheit und des technischen Datenschutzes muss deshalb durch Stärkung von Expertisen erheblich mehr Aufmerksamkeit geschenkt und der präventive Aufwand – personell und sachlich – deutlich erhöht werden.

Neue Ziele braucht das Land

Aber es muss neben einer solchen praktischen Korrektur im Alltag der IT-Verfahrensentwicklung und -pflege noch etwas Grundlegendes in Frage gestellt werden: das System der Schutzziele. Bereits die Europäische Datenschutzrichtlinie kennt die vier Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit und Prüfbarkeit. Das Bundesverfassungsgericht hat 2008 zwei dieser Ziele mit Verfassungsrang ausgestattet und entschieden, dass das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. Die Nennung von nur zwei Schutzzielen in diesem Urteil schließt jedoch nicht aus, dass das Gesamtmodell der Schutzziele einer umfassenderen Weiterentwicklung unterzogen werden muss, denn um der Komplexität heutiger und künftiger Systeme gerecht zu werden, müssen die Ziele insgesamt abstrakter gefasst und technikneutral formuliert werden, als dies im NDSG mit den aktuellen Kontrollzielen der Fall ist.

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

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSB-Konferenz) hat sich in einer Arbeitsgruppe intensiv mit der Neufassung der Technikregelung in § 9 BDSG (und damit auch mit der des § 7 NDSG) befasst. Mein Technikteam hat in dieser Arbeitsgruppe ebenfalls mitgewirkt.

Für die Neufassung der technisch-organisatorischen Regelungen in den Datenschutzgesetzen galten folgende Rand- und Rahmenbedingungen:

1. Grundlage sollte die Definition elementarer Schutzziele sein, aus denen sich weitere (Schutz-) Ziele systematisch herleiten lassen, die einfach, verständlich und praxistauglich sein sollen.
2. Die Schutzziele sollten somit soweit wie möglich den elementaren Schutzzielen der IT-Sicherheit (Verfügbarkeit, Unversehrtheit/Integrität, Vertraulichkeit) entsprechen und/oder zumindest mit ihnen korrespondieren und Überschneidungspunkte aufweisen, dabei jedoch die speziellen Anforderungen des Schutzes personenbezogener Daten zum Tragen kommen lassen.

3. Die Schutzziele müssen an den Vorgaben des Datenschutzes gemessen werden und über längere Zeit bestand haben.
4. Auf der Basis der Schutzziele sollte sich ein Katalog von konkreten Datenschutzmaßnahmen ableiten lassen. Dieser Maßnahmenkatalog sollte – ähnlich dem Ansatz des IT-Grundschutzkataloges des Bundesamtes für Sicherheit in der Informationstechnik – in ein flexibles, einfaches, praxistaugliches und durch Software unterstütztes Verfahren münden können. Dieses Verfahren auf der Schutzzielebasis sollte als Kriterien-Katalog eines Datenschutzaudits herangezogen werden können.
5. Die elementaren Schutzziele sollen technologieunabhängig definiert werden.
6. Die Nachhaltigkeit der Schutzziele muss gewährleistet sein; das heißt, dass bei zukünftigen technischen Systemen das Modell der Schutzziele vollständig, ausreichend und weiterhin gültig bleibt. Das bedeutet auch, dass die Ausgestaltung dieser Schutzziele mittels technischer und organisatorischer Maßnahmen und deren Fortschreibung das IT-System zu jedem Zeitpunkt eine datenschutzkonforme Verarbeitung sicherstellen muss. Somit gilt: Die Schutzziele bleiben, die Maßnahmen müssen sich dagegen weiterentwickeln.
7. Grundsätzliche rechtliche Anforderungen (z. B. Datenvermeidung, Datensparsamkeit, Zweckbindung, Betroffenenrechte wie Auskunft, Berichtigung und Löschung) müssen möglichst technisch durchgesetzt werden. Dies greift das Konzept Systemdatenschutz und Datenschutz durch Technik auf (Privacy Enhancing Technology, PET):
   - Löschbarkeit muss implementierbar sein.
   - Betroffenenrechte (z. B. Auskunfts-, Berichtigungs- und Löschungsansprüche) müssen technisch umsetzbar sein.
   - Identitätsmanagement (Anonymisierung und Pseudonymisierung) muss implementiert sein.
   - Revisionsfeste Protokollierung muss implementiert sein.

Privacy Enhancing Technology, PET: „Verkettung digitaler Identitäten", Report des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, 31.07.2007, www.datenschutzzentrum.de/projekte/verkettung

Die technisch-organisatorischen Maßnahmen, die sich aus dem sich wandelnden technischen Fortschritt ergeben, sowie datenschutzfreundliche Techniken müssen angemessen abgebildet werden können. Das gilt insbesondere für die Durchsetzung der Entkettbarkeit von verkoppelten Systemen (z. B. bei Data Warehouse Systemen, virtuellen IT-Systemen, Cloud Computing oder Webservices).
Technisch-organisatorische Regelungen müssen die Grundlage für ein Datenschutzaudit liefern können.

Sechsfach zukunftsfähig

Unter diesen Rahmenbedingungen definierte der Arbeitskreis folgenden Katalog von sechs Schutzzielen des technisch-organisatorischen Datenschutzes:
Verfügbarkeit: Verfahren und Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß angewendet werden.
Vertraulichkeit: Auf Verfahren und Daten darf nur befugt zugegriffen werden.
Integrität: Daten aus Verfahren bleiben unversehrt, zurechenbar und vollständig.
Transparenz: Erhebung, Verarbeitung und Nutzung personenbezogener Daten müssen mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden können.

Unverkettbarkeit: Verfahren sind so einzurichten, dass deren Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (technisch-organisatorische Gewährleistung der Zweckbindung).
Intervenierbarkeit: Verfahren sind so zu gestalten, dass sie dem Betroffenen die Ausübung der ihm zustehenden Rechte wirksam ermöglichen.

Diese sechs Ziele und die daraus abgeleiteten technischen und organisatorischen Maßnahmen sind als ein zusammenhängendes Schutzsystem zu verstehen, Eine große Zahl dieser Datenschutzmaßnahmen entfalten gleichzeitig ihre Wirkung in der IT-Sicherheit, also bei der Sicherung des Betriebsablaufs. Deshalb gibt es zwischen dem Datenschutzkonzept und den sonstigen Sicherheitskonzepten einen engen Zusammenhang. Aus meiner Erfahrung ist es daher auch sinnvoll, bei IT-Projekten die IT-Sicherheitskonzepte einerseits und die Vorabkontrolle und die Datenschutzkonzepte andererseits zeitlich parallel zu entwickeln, um die Überschneidungen, Wechselwirkungen und Abstimmungserfordernisse rechtzeitig und sachgerecht zu gestalten.
Im Ergebnis wurde der neue Schutzzielekatalog vom Arbeitskreis Technik im Frühjahr 2010 verabschiedet und durch die 79. DSB-Konferenz mit einer Entschließung in ihrem Eckpunktepapier für die Modernisierung des Datenschutzrechtes am 18.3.2010 berücksichtigt.

Sichere Informationstechnik gewinnt immer mehr an Bedeutung

Die Umsetzung dieses Schutzzielekataloges halte ich für eine wichtige Fortentwicklungsmaßnahme in der Rechtssetzung. Dies ist Voraussetzung dafür, dass die Datenschutzbestimmungen für die aktuellen Herausforderungen der Informationstechnik gewappnet sind. Den immer zahlreicheren Angriffen auf digitale Informationen der Bürgerinnen und Bürger und damit auf deren Persönlichkeitsrechte kann nur begegnet werden, wenn die Definition der Schutzziele technikneutral auf alle neuen Szenarien anwendbar ist. Das gilt erst recht für die schnelllebigen Innovationen im Bereich von mobilen Endgeräten (Smartphones, Ortungsdienste, Tablet-PC etc.), des Internets und des Cloud Computings. Gerade die Allgegenwärtigkeit von Computern in Alltagsgegenständen (so genanntes ubiquitäres Computing) wird sich weiter verdichten. Die Komplexität der Systeme und die Vielzahl der bewussten, der unbewussten und sogar der unbemerkten Datenströme werden weiter extrem steigen. Damit wird auch die Zahl der Gefährdungen für personenbezogene Daten weiter ansteigen. Ich rechne nicht mit einem Rückgang der Sicherheitsvorfälle. Ich befürchte allerdings einen gewissen Gewöhnungseffekt im Zusammenhang mit Datenschutzskandalen. Es wäre fatal, dies als Normalisierung zu interpretieren. Ich hielte dies eher für einen Ausdruck kollektiver Selbstaufgabe hinsichtlich elementarer Grundrechte, der Persönlichkeitsrechte und letztlich des Menschenbildes.
Deshalb muss die Sicherheit der Informationstechnik auch in der Zukunft durch ein verbessertes System von Schutzzielen im Gesetz verankert sein – ein aus meiner Sicht dringender gesetzgeberischer Reformbedarf für Bundestag und Landtag. Eine Berücksichtigung der Beschlüsse der DSB-Konferenz im Gesetzgebungsverfahren steht unterdessen leider noch aus.

Weitere Informationen:

„Modernisierung des Datenschutzrechts“ und Anlage 2
www.lfd.niedersachsen.de
Pfad: Home > Allgemein > DSB-Konferenzen > Pressemitteilungen > Frühjahrskonferenz 2010

IT-Management des Landes: Der Landesdatenschutzbeauftragte berät

Bis zur Errichtung des so genannten IT-Planungsrates im Jahre 2010 war die strategische Führung für das Management der Informations- und Kommunikationstechnik der niedersächsischen Landesverwaltung in zwei Zuständigkeiten geteilt. Nach den „Grundsätzen zur Steuerung und Koordinierung des Einsatzes der Informations- und Kommunikationstechnik in der Landesverwaltung (SK-IT)" oblag dem Ministerium für Inneres und Sport die Federführung: Das „Zentrale IT-Management (ZIM)" hatte hierbei die zentralen Aufgaben der Steuerung, Koordinierung und des Controlling des IT-Einsatzes wahrzunehmen. Der Koordinierungsausschuss IT (KA-IT) diente dagegen als Beratungs- und Beschlussgremium der ressortübergreifenden Koordination und Abstimmung. Er beriet über alle Fragen von grundsätzlicher Bedeutung für den IT-Einsatz in der Landesverwaltung und wirkte bei den strategischen Vorgaben mit. Bei der Aufstellung und Fortschreibung des IT-Landeskonzepts, der Grundsätze der Aufstellung des IT-Gesamtplans und der Grundsätze der Durchführung des landeszentralen IT-Controllings war der KA-IT zu beteiligen.

Grundsätze zur Steuerung und Koordinierung des Einsatzes der Informations- und Kommunikationstechnik in der Landesverwaltung (SK-IT), Gem. RdErl. d. MI, d. StK u.d. übr. Min. v. 7.9.2004 – VM 501-02828/3-2 – vom 7. September 2004 (Nds. MBl. S. 563)

Neben meiner Kontrollfunktion (§ 22 Abs. 1 Satz 1 NDSG) gegenüber öffentlichen Stellen kommt der frühzeitigen Mitwirkung mit beratender Funktion (§ 22 Abs. 1 Satz 3 NDSG) bei solchen Planungen eine besondere Bedeutung zu. Als beratendes Mitglied hat der in meiner Geschäftsstelle für technischen Datenschutz zuständige Teamleiter im Berichtszeitraum an allen Sitzungen und Sondersitzungen in diesem Gremium mitgewirkt.
Er gab inhaltlich häufig präventive Hinweise aus materiellrechtlicher und technisch-organisatorischer Sicht des Datenschutzes zu verschiedenen E-Government-Verfahren im Rahmen des Masterplans, zu zahlreichen Aspekten der IT-Konsolidierung und den Migrations- und Transformationsprozessen im Rahmen der von der Landesregierung seit 2005 beschlossenen Verwaltungsmodernisierung sowie insbesondere zu IT-Sicherheitsstrategien, -prozessen und -maßnahmen. Die Zusammenarbeit war dabei fast ausschließlich positiv zu bewerten. Beratungsaspekte wurden stets konstruktiv aufgegriffen.
Doch nicht alle Empfehlungen wurden umgesetzt. Das trifft insbesondere auf die Outsourcing- und Outtasking-Strategien zu, die angesichts der deutlichen Gefahren für IT-Verfahren hoheitlich agierender Verwaltungsbereiche eine erheblich kritischere Einschätzung verdienen. Aktuell sind mindestens zwei Großprojekte von dieser Problematik betroffen: das Storage Management/Managed Storage im LSKN und das geplante Desktop Management für die Landesverwaltung.

Föderalismusreform führte zum IT-Planungsrat

Die alte Organisation wurde 2010 in der Folge von Aufgabenänderungen, die sich aus der Änderung des Grundgesetzes (GG) im Rahmen der Föderalismusreform ergeben hatten, aufgehoben. Dies führte auch zu einer Anpassung der Präventionsaufgaben meiner Geschäftsstelle.
Artikel 91c GG regelt seit 2009 eine engere Koordination im IT-Management von Bund und Ländern. Hiernach können
„[...] Bund und Länder bei der Planung, der Errichtung und dem Betrieb der für ihre Aufgabenerfüllung benötigten informationstechnischen Systeme zusammenwirken.

Zudem können Bund und Länder auf Grund von Vereinbarungen die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen."

Diese engere Zusammenarbeit hat auch Auswirkungen auf die praktische länderseitige Gestaltungsfreiheit der Regularien und die verfahrensbestimmenden Architekturentscheidungen für E-Government, insbesondere auf IT-Standards, Schnittstellen und Innovationsentscheidungen. Das kann einerseits einschränkend und bindend sein, andererseits eröffnet es auch die Möglichkeit der Mitgestaltung und Einflussnahme auf bundeseinheitliche Entscheidungen. Nicht zuletzt aber bietet es die Chance zur Standardisierung auf höherem Niveau. Diese Entscheidungen wirken sich unmittelbar auf das Niveau der IT-Sicherheit und des technisch-organisatorischen Datenschutzes aus. Gleichzeitig ist bei den verfassungsrechtlich abgesicherten schutzwürdigen Persönlichkeitsrechten darauf zu achten, dass solche Entscheidungen datenschutzfördernd getroffen werden und dass Standards und Sicherheitsanforderungen auch den Datenschutz aktiv befördern.

Große IT-Projekte führen oft zu neuen Datensammlungen

Erfahrungsgemäß sind die Hauptmotivation von ehrgeizigen IT-Verfahren und neuen Technologien aber die Wirtschaftlichkeit, die Verbesserung der Bürgernähe und die Beschleunigung von Verfahrensabläufen. Ein Hauptaugenmerk liegt stets auf der Einsparung von Personalkosten, um zur Konsolidierung öffentlicher Haushalte beizutragen. Daher verwundert es auch nicht, dass große IT-Projekte stets neue Verknüpfungen von Verfahren oder sogar neue Datensammlungen hervorbringen. Hier liegen jedoch auch die altbekannten Interessenkollisionen mit dem datenschutzrechtlichen Grundsatz der Datensparsamkeit.

Artikel 91c GG weist jedoch nun eine Besonderheit auf. Es heißt dort:
„Die Vereinbarungen über die Grundlagen der Zusammenarbeit nach Satz 1 können für einzelne nach Inhalt und Ausmaß bestimmte Aufgaben vorsehen, dass nähere Regelungen bei Zustimmung einer in der Vereinbarung zu bestimmenden qualifizierten Mehrheit für Bund und Länder in Kraft treten. Sie bedürfen der Zustimmung des Bundestages und der Volksvertretungen der beteiligten Länder; das Recht zur Kündigung dieser Vereinbarungen kann nicht ausgeschlossen werden. [...]"

Die durch diese qualifizierte Mehrheit zustande kommenden Regelungen sind fortan für alle Länder bindend. Die bundeseinheitliche Verbindlichkeit der Entscheidungen ist schwerer korrigierbar. Aber die Stringenz in der Verkettung komplexer technischer, rechtlicher und organisatorischer Aspekte bietet auch die Chance zu höherer Qualität. Sie engt aber gleichzeitig die Spielräume ein. Und nicht zuletzt stellt sie die Datenschutzbeauftragten des Bundes und der Länder vor neue zeitliche und quantitative Herausforderungen, weil die Koordinierung der datenschutzrechtlichen Stellungnahmen aller Beteiligten in einem zeitlich engeren Rahmen und gleichzeitig auf komplexerem Wege gelingen muss.
Noch stärker ausgeprägt ist die Verbindlichkeit und Stringenz bei der Festlegung von Infrastrukturinvestitionen wie etwa bei IT-Netzen. Nach Artikel 91c Grundgesetz ist vorgesehen:

„Die Länder können darüber hinaus den gemeinschaftlichen Betrieb informationstechnischer Systeme sowie die Errichtung von dazu bestimmten Einrichtungen vereinbaren.
Der Bund errichtet zur Verbindung der informationstechnischen Netze des Bundes und der Länder ein Verbindungsnetz."

Gesetz regelt Verbindungsnetz

Von der verfassungsrechtlich vorgesehenen Möglichkeit, Errichtung und Betrieb des Verbindungsnetzes durch ein Bundesgesetz zu regeln, hat der Bund 2009 mit dem Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG) Gebrauch gemacht.
Für die Umsetzung der Änderung der „Planungshoheit" bedurfte es jedoch einer weiteren gesetzlichen Grundlage. Der Bund und alle 16 Bundesländer unterzeichneten daher 2009 einen entsprechenden Staatsvertrag, den „Vertrag über die Errichtung des IT-Planungsrates und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG". Danach gibt es ein zentrales Planungsgremium (Abschnitt I § 1 Abs. 1):
Der Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (IT-Planungsrat)

1. koordiniert die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik,
2. beschließt fachunabhängige und fachübergreifende IT-Interoperabilitäts- und IT-Sicherheitsstandards,
3. steuert die Projekte zu Fragen des informations- und kommunikationstechnisch unterstützten Regierens und Verwaltens (E-Government-Projekte), die dem IT-Planungsrat zugewiesen werden,
4. übernimmt die in § 4 dieses Vertrages genannten Aufgaben für das Verbindungsnetz nach Maßgabe des dort angeführten Gesetzes.

Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder – Gesetz zur Ausführung von Artikel 91c Absatz 4 des Grundgesetzes – vom 10.08.2009 (IT-NetzG), BGBl I, S. 2706

Staatsvertrag: Vertrag über die Errichtung des IT-Planungsrates und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG vom 30. Oktober und 20. November 2009

Nds. Gesetz zum Staatsvertrag über die Errichtung des IT-Planungsrates und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG vom 17.03.2010 (Nds. GVBl, Seite 142)

www.it-planungsrat.de

Der IT-Planungsrat löst seither die bisherigen Gremien der Bund-Länder übergreifenden IT-Steuerung, den Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern und den Kooperationsausschuss von Bund und Ländern für automatisierte Datenverarbeitung (KoopA ADV) sowie alle Untergremien ab. Der Niedersächsische Landtag hat mit Gesetz vom 17.3.2010 diesen Staatsvertrag als geltendes Landesrecht verabschiedet.

Staatsvertrag überträgt Planungshoheit auf IT-Planungsrat

Während einer längeren Phase der Konstituierung des IT-Planungsrates stand auch die Frage zur Diskussion, inwieweit die Datenschutzfragen bei IT-Planungen hinreichend Berücksichtigung finden. Nach § 1 Abs. 2 Satz 2 des Vertrages wurde dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine

optionale Teilnahme mit beratender Stimme eingeräumt. Nach eingehender Erörterung setzte sich jedoch die Erkenntnis durch, dass das Datenschutzrecht in vielfältigen Landesnormen verankert ist und deshalb mindestens eine zusätzliche beratende Stimme aus der Länderebene erforderlich ist. Die Datenschutzbeauftragten von Bund und Ländern einigten sich auf ein bewährtes Konstrukt: Als Sprecher für die Länder sollte der Vorsitzende des Arbeitskreises „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten von Bund und Ländern (DSB-Konferenz), der LfDI Mecklenburg-Vorpommern, an den Sitzungen mit beratender Stimme teilnehmen. Der IT-Planungsrat folgte diesem Vorschlag. Seither besteht die Möglichkeit, dass auch von meiner Seite, insbesondere aus der fachlichen Beurteilung von E-Government-Verfahren und des technisch-organisatorischen Datenschutzes, Stellungnahmen über meinen Kollegen in Mecklenburg-Vorpommern beigesteuert werden können.
Neben den Befassungen zu organisatorischen Fragen der Selbstkonstituierung und Untergremienbeauftragung gab es im Berichtszeitraum inhaltliche Entscheidungen des IT-Planungsrates in den ersten drei Sitzungen im Jahre 2010 insbesondere zu folgenden Themen und Projekten:

- Nationale E-Government-Strategie,
- Einheitliche Behördennummer D115,
- Kfz-Wesen,
- DOI Netz e.V.,
- IT im Bereich Grundsicherung für Arbeitssuchende (SGB II),
- Kooperationsgruppe Nationale E-Government-Strategie,
- Aufbau der Koordinierungsstelle für IT-Standards,
- Konsolidierter Projekt- und Anwendungsplan,
- Ansprechpartner für EU-Gremium.

Bildung eines Niedersächsischen IT-Planungsrates

Parallel zu der Neukonstituierung des IT-Planungsrates auf Bund-Länder-Ebene war es folgerichtig, auf der Landesebene ein organisatorisches Gegenstück zu schaffen. Da der o. g. Staatsvertrag die Rahmenbedingungen verändert hatte und der Bund und die Länder sicherzustellen haben, dass ihre Vertreter über die erforderliche Entscheidungskompetenz verfügen (Prinzip des einheitlichen Mandates je Land, § 1 Abs. 2 Satz 2 des Vertrages), war es erforderlich geworden, dieses einheitliche Mandat mittels eines Landesgremiums zu etablieren.
Die Landesregierung hat die Einrichtung eines Niedersächsischen IT-Planungsrates zum 1. April 2010 beschlossen. Mit dem Niedersächsischen IT-Planungsrat sollen – unter Vorsitz des IT-Bevollmächtigten der Landesregierung (CIO) im Nds. Ministerium für Inneres und Sport – die zukünftigen Anforderungen, die aus dem IT-Planungsrat Bund/Länder auf das Land zukommen, bewältigt werden. Insbesondere soll eine ausgereifte landesinterne Abstimmung ermöglicht werden, wenn Beschlussvorschläge auf Bund/Länder-Ebene herbeizuführen sind, insbesondere wenn die Angelegenheiten mehrerer niedersächsischer Ministerien (§ 22 GGO) oder Interessen der Kommunen berührt sind. Außerdem soll die Landesregierung in ihren Kabinettssitzungen entlastet werden, indem die fachlichen Beurteilungen einem hohen Gremium übertragen wird. Daher werden einstimmige verbindliche Beschlüsse des Nds. IT-Planungsrates angestrebt, die unter Einbindung aller Ministerien und eines Vertreters der kommunalen Spitzenverbände gefasst werden. Neu ist auch, dass abschließende Entscheidungen, also verbindliche Festlegungen über das Abstimmverhalten des Landesvertreters im IT-Planungsrat Bund/Länder getroffen werden, um das Mandat zu festi-

gen. Der Nds. IT-Planungsrat hat außerdem über Festlegungen zur Umsetzung von Beschlüssen des IT-Planungsrats Bund/Länder sowie über fachunabhängige und fachübergreifende IT-Interoperabilitäts-und IT-Sicherheitsstandards für Niedersachsen zu entscheiden.

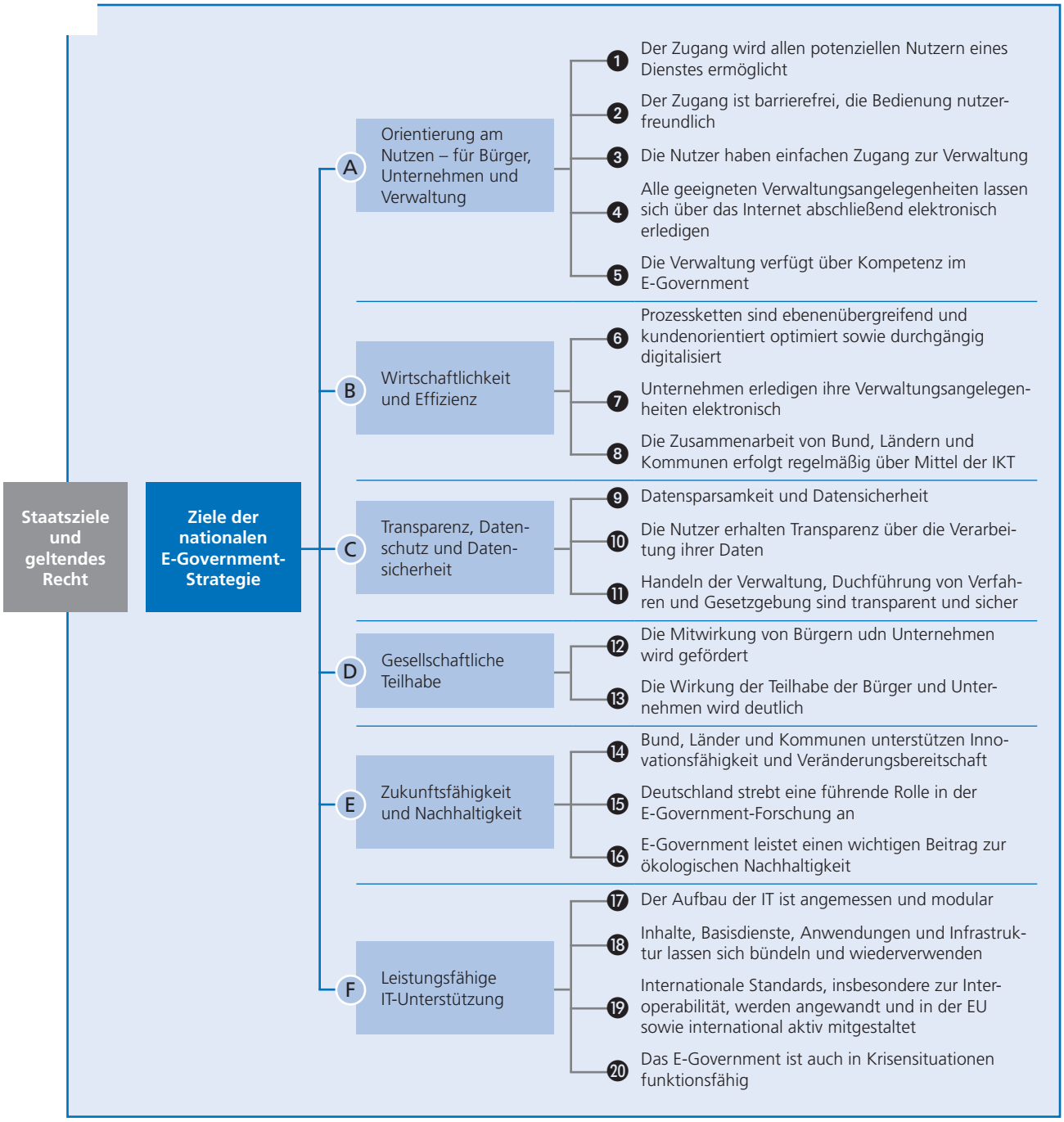
Herausforderungen für den materiellrechtlichen und technisch-organisatorischen Datenschutz

Hier eröffnen sich grundlegende Felder, die in erheblicher Größenordnung – quantitativ wie auch qualitativ – Fragen und Herausforderungen für den materiellrechtlichen und technisch-organisatorischen Datenschutz nach sich ziehen. Dieser Bereich muss durch meine Behörde präventiv begleitet werden und unterliegt meiner gesetzlichen Aufsichtsfunktion. Schließlich muss der Nds. IT-Planungsrat die ressortübergreifende Koordination und Abstimmung des IT-Einsatzes sicherstellen.
Stimmberechtigte Mitglieder sind der IT-Bevollmächtigte der Landesregierung, jeweils eine Vertreterin oder ein Vertreter jedes Ressorts sowie zusätzlich der Haushaltsabteilung des Finanzministeriums. Beratende Mitglieder sind jeweils eine Vertreterin oder ein Vertreter der kommunalen Spitzenverbände, der Landtagsverwaltung, des Landesbeauftragten für den Datenschutz, des Landesbetriebs für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) und des Landesrechnungshofes. Damit ist sichergestellt, dass auch in diesen Entscheidungsstrukturen für die Zukunft die präventiv-beratende Funktion des LfD in Fällen von strategischen und wichtigen operativen IT-Planungen direkt vor den Entscheidungen erfolgen kann.

Kapazitätsprobleme

Die Bandbreite der Themen, die Zahl der großen IT- und E-Government-Verfahren und die großen Infrastruktur- und IT-Sicherheitsprojekte binden bereits jetzt erhebliche personelle Ressourcen in meiner Behörde. Eine deutliche Steigerung und Intensivierung war hier bereits im Berichtszeitraum erkennbar. Eine weitere Steigerung und Intensivierung begleitender Arbeiten ist auch für die Zukunft dringend erforderlich, denn die Anforderungen werden quantitativ deutlich ansteigen.
Zusätzlich zur beschriebenen Gremienarbeit auf der Bund-/Länder-Ebene und der Landesebene sind zur Unterstützung des IT-Planungsrates derzeit vier Untergremien eingesetzt: die Koordinierungsstelle für IT-Standards (KoSIT), Kooperationsgruppe Strategie, Kooperationsgruppe EU und Kooperationsgruppe Leitlinie Informationssicherheit. Um die Datenschutzfragen in diesen operativen Gremien ebenfalls rechtzeitig präventiv-beratend seitens der Datenschutzbeauftragten des Bundes und der Länder begleiten zu können, wäre eine Gremienmitarbeit erforderlich und sinnvoll. Diese weitere Bindung von Personalressourcen ist jedoch bei der Personalausstattung der Datenschutzbehörden nicht darstellbar. Ich halte mittelfristig eine entsprechende Verstärkung in diesem Bereich für unverzichtbar.

Zielsystem der nationalen E-Government-Strategie



Quelle: BMI, IT-Planungsrat

Weitere Informationen:

www.mi.niedersachsen.de
Pfad: Home > Themen > Verwaltungsmodernisierung & Organisation der Landesverwaltung > Verwaltungsmodernisierung („Neuausrichtung der IT“)
www.lskn.niedersachsen.de
www.lfd.niedersachsen.de
Pfad: Home > Technik und Organisation

Vorratsdaten: Totalspeicherung ohne Anfangsverdacht

Nur wenige andere Themen haben in der Geschichte des Datenschutzes so lang andauernd und intensiv zu gesellschaftlichen und rechtspolitischen Auseinandersetzungen geführt wie die Kontroverse zur so genannten Vorratsdatenspeicherung. Dabei scheint es, dass die Komplexität der Materie eine große Rolle spielt. Auch die extreme und unversöhnliche Gegensätzlichkeit der Rechtsdogmen ist ein Grund, denn bei aller Streitigkeit über die Qualität dieser Datensammlung zwischen Strafprozessrecht einerseits und freier Mediennutzung und Privatsphäre andererseits muss sich jede gesetzliche Lösung am Verfassungsrecht und am europäischen Menschenrechtsrahmen messen lassen.

EU-Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.03.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:DE:HTML

In der Sache geht es nach wie vor um nicht weniger als eine Totalspeicherung aller Verbindungsinformationen über einen langen Zeitraum, die sämtliche Telekommunikationsnutzer bei allen Vorgängen erzeugen. Die Vorratsdatenspeicherung sollte über die Verknüpfung aller Telekommunikationsarten (Festnetz- und Mobiltelefonie, Standortdaten, SMS, E-Mail und Internet) die Erstellung von Kommunikationsprofilen ermöglichen, um Terrorismus und andere schwere Straftaten besser bekämpfen zu können. Alle Datenschutzbeauftragten des Bundes und der Länder haben sich stets gegen diese Datensammlung ausgesprochen. Mit der Entscheidung des Bundesverfassungsgerichtes 2010[1] ist die politische Debatte jedoch nicht beendet. Es lohnt sich daher durchaus, zum besseren Gesamtverständnis zeitlich weiter auszuholen. So ist vorauszuschicken, dass einst (2004/2005) von allen Fraktionen des Deutschen Bundestages eine anlasslose und umfassende Vorratsdatenspeicherung im Vorfeld der EU-Richtlinie einstimmig und mit Nachdruck abgelehnt worden war.[2]

EU-Vorgabe 2006: Anlassunabhängige Massenspeicherung von Telekommunikations-Verkehrsdaten

Das Nein im Bundestag war aber kein Schlussstrich unter diesem Thema. Innerhalb weniger Monate verabschiedete das Europäische Parlament 2006 die Richtlinie zum Erfassen von Telekommunikationsverbindungsdaten. Die Mitgliedstaaten wurden darin verpflichtet, die Regelung bis zum 15.9.2007 in nationales Recht umzusetzen, also die Rechts- und Verwaltungsvorschriften in Kraft zu setzen, die erforderlich sind, um dieser Richtlinie bis zu diesem Termin nachzukommen. Es ging hier um die EU-weite Harmonisierung von Rechtsvorschriften und inhaltlich um die für die Strafverfolgung für erforderlich gehaltene verdachtsunabhängige Speicherung der Telekommunikations-Verkehrsdaten, die so genannte

1 Urteil des BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08)

2 Drucksache 15/4597 vom 22. 12. 2004, Nr. 8 der Beschlussempfehlung und des Berichts des Bundestags-Innenausschusses (4. Ausschuss) zur Unterrichtung durch den Bundesbeauftragten für den Datenschutz (Drucksache 15/888) zum 19. BfDI-Tätigkeitsbericht 2001 und 2002 (http://dipbt.bundestag.de/dip21/btd/15/045/1504597.pdf), einstimmig vom Deutschen Bundestag angenommen am 17. Februar 2005 (Plenarprotokoll Seite 14733, http://dipbt.bundestag.de/dip21/btp/15/15157.pdf)

Vorratsdatenspeicherung. Eine verdachtsunabhängige Speicherung bedeutet, dass die Speicherung erfolgt, ohne dass ein Anfangsverdacht oder konkrete Hinweise auf Gefahren bestehen. Der vorgegebene Rahmen der Richtlinie umfasste eine Speicherdauer von sechs bis 24 Monaten.
Mit Stand August 2011 war die Richtlinie in fünf von 27 Mitgliedstaaten nicht umgesetzt.

2007: Frühzeitige Warnung der DSB-Konferenz

Zahlreiche kritische Stimmen insbesondere aus der Bürgerrechtsbewegung, einiger Medien, aber auch aus dem politischen Raum begleiteten den Gesetzgebungsprozess über Jahre hinweg und erhoben Zweifel an der Richtigkeit und Verfassungsmäßigkeit einer solchen Regelung. Auch die Datenschutzbeauftragten des Bundes und der Länder nahmen von Anfang an eine kritische Haltung ein. „Vorratsdatenspeicherung, Zwangsidentifikation im Internet, Telekommunikationsüberwachung und sonstige verdeckte Ermittlungsmaßnahmen", unter diesem Titel nahm die 73. Konferenz in ihrer Sitzung im März 2007 in Erfurt bereits zu dem ersten Referentenentwurf mit einer Entschließung Stellung. Insbesondere wurde die vorgesehene Kernbereichsregelung für ungenügend gehalten. Sie nehme in Kauf, dass regelmäßig auch kernbereichsrelevante Informationen erfasst würden, für die aber grundsätzlich ein Erhebungsverbot gelten müsse. Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung, die dennoch erlangt würden, müssten zudem einem absoluten Verwertungsverbot unterliegen, forderte die Konferenz. Außerdem wies sie darauf hin, dass für die Kommunikation mit Berufsgeheimnisträgern ein absolutes Erhebungs- und Verwertungsverbot geschaffen werden sollte, das dem jeweiligen Zeugnisverweigerungsrecht entspricht. Dieses sollte unterschiedslos für alle Berufsgeheimnisträgerinnen und Berufsgeheimnisträger und deren Berufshelferinnen und -helfer gelten.

Meine Presseerklärung vom 12.03.2007 unter: www.lfd.niedersachsen.de
Pfad: Home > Allgemein > Aktuelles > Presseinformationen > Archiv > Frühjahrskonferenz der Datenschutzbeauftragten des Bundes und der Länder in Erfurt

Die DSB-Konferenz machte weitere Kritikpunkte in dieser Entwurfsphase zum TKG geltend:

- Für Angehörige i. S. v. § 52 StPO sollte ein Erhebungs- und Verwertungsverbot für die Fälle vorgesehen werden, in denen das öffentliche Interesse an der Strafverfolgung nicht überwiegt. Die besonderen verwandtschaftlichen Vertrauensverhältnisse dürften nicht ungeschützt bleiben.
- Für teilnehmende Personen von Kernbereichsgesprächen, die weder Berufsgeheimnisträgerinnen und Berufsgeheimnisträger noch Angehörige i. S. v. § 52 StPO sind, sollte ein Aussageverweigerungsrecht aufgenommen werden. Andernfalls bliebe der Kernbereich teilweise ungeschützt.
- Für die so genannten Funkzellenabfrage, die alle Telefonverbindungen im Bereich einer oder mehrerer Funkzellen erfasst, sollten klare und detaillierte Regelungen mit engeren Voraussetzungen normiert werden. Diese sollten vorsehen, dass im Rahmen einer besonderen Verhältnismäßigkeitsprüfung die Anzahl der durch die Maßnahmen betroffenen unbeteiligten Dritten berücksichtigt und die Maßnahme

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter:
www.lfd.niedersachsen.de
Pfad: Allgemein > DSB-Konferenzen > Entschließungen

auf den räumlich und zeitlich unbedingt erforderlichen Umfang begrenzt wird. Die Unzulässigkeit der Maßnahme zur Ermittlung von Tatzeuginnen und Tatzeugen sollte ins Gesetz aufgenommen werden.

- Die aufgrund einer Anordnung der Staatsanwaltschaft bei Gefahr in Verzug erlangten Daten dürften nicht verwertet werden, wenn die Anordnung nicht richterlich bestätigt wird. Dieses Verwertungsverbot darf nicht - wie im Entwurf vorgesehen - auf Beweiszwecke begrenzt werden.
- Art und Umfang der Begründungspflicht für den richterlichen Beschluss der Anordnung der Telekommunikationsüberwachung sollte wie bei der Wohnraumüberwachung im Gesetz festgeschrieben werden. Im Sinne einer harmonischen Gesamtregelung sollten darüber hinaus qualifizierte Begründungspflichten für sämtliche verdeckte Ermittlungsmaßnahmen geschaffen werden.
- Zur Gewährleistung eines effektiven Rechtsschutzes ist sicherzustellen, dass sämtliche Personen, die von heimlichen Ermittlungsmaßnahmen betroffen sind, nachträglich von der Maßnahme benachrichtigt werden, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Darüber hinaus sollte bei Massendatenerhebungen über eine ergänzende Benachrichtigung durch eine öffentliche Bekanntmachung der Maßnahme nachgedacht werden.
- Die für die Telekommunikationsüberwachung vorgesehenen Berichts- und Statistikpflichten sollten um Angaben zur Dauer der Überwachung, zur Anzahl der Gespräche und zur Benachrichtigung Betroffener ergänzt werden.
- Die im Entwurf enthaltenen erweiterten Eingriffsgrundlagen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden.

2007/2008: Gesetzgeber beschließt trotz Kritik umfassende Datensammlung

Deutschland setzte die Vorgabe der Richtlinie durch die Verabschiedung eines Änderungsgesetzes zum Telekommunikationsgesetz (TKG) um. Bundestag[3] und Bundesrat[4] verabschiedeten 2007 ungeachtet der Kritikpunkte diese für Bürgerinnen und Bürger sowie Provider verpflichtenden und dabei tief in die Persönlichkeitsrechte jedes einzelnen Bürgers eingreifenden Normen. Bemerkenswert war, dass eine Reihe von Abgeordneten zwar dem Gesetz zustimmte, jedoch in einer Erklärung ausdrücklich „schwerwiegende politische und verfassungsrechtliche Bedenken" hatte.[5] Basierend auf dem von der Bundesregierung vorgelegten „Gesetzentwurf zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG"[6] wurden neben der Änderung verschiedener Rechtsvorschriften (u. a. Strafprozessordnung, Telekommunikationsgesetz, Abgabenordnung, Strafgesetzbuch, Artikel 10-Gesetz, BKA-Gesetz, Telekommunikations- Überwachungsverordnung) insbesondere der § 113 a TKG („Speicherungspflichten für Daten") und § 113 b TKG („Verwendung der nach § 113 a gespeicherten Daten") als Eingriffsnormen für die Ermittlungsbehörden hinzugefügt.[7]

3 Namentlicher Abstimmung im Bundestag am 09.11.2007 (http://webarchiv.bundestag.de/archive/2009/1022/bundestag/plenum/abstimmung/20071109_teleueberwach.pdf)

4 Beschluss der 839. Sitzung des Bundesrates am 30.11.2007, Drucksache 798/07(B) (http://www.bundesrat.de/cln_179/nn_45602/SiteGlobals/Forms/Suche/beratungsvorgangssucheNavigation__Formular,templateId=processForm.html?__nnn=true)

5 Stenografischer Bericht zur 124. Plenarsitzung des Deutschen Bundestages vom 09.11.2007 (http://dipbt.bundestag.de/dip21/btp/16/16124.pdf#P.13005)

6 Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" vom 27. 06. 2007, Drucksachen 16/5846 und 16/6979 (http://dipbt.bundestag.de/dip21/btd/16/058/1605846.pdf)

7 Das Gesetz vom 21.12.2007 wurde verkündet am 31.12.2007 im Bundesgesetzblatt Teil I 2007 Nr. 70 31.12.2007 S. 3198

2008:
DSB-Konferenz fordert neue Datenschutzkultur

Auch wenn selbstverständlich den Erfordernissen der Strafverfolgungsbehörden in einer rechtsstaatlichen Ordnung angemessen Rechnung zu tragen ist, sind Einschränkungen grundgesetzlich geschützter Interessen im Wege der Güterabwägung auf das zur Sicherung der Belange von Strafverfolgung unabdingbare Maß zu begrenzen. Unter dieser Prämisse war diese Gesetzgebung für den Grundrechtsschutz als grundlegend problematisch einzuordnen.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sah dies ähnlich und zeigte sich in der so genannten „Berliner Erklärung" im April 2008 äußerst besorgt über die Vorratsdatenspeicherung im Kontext mit zahlreichen zusätzlichen Eingriffsnormen für den Staat und einer zunehmenden verfassungsrechtlichen Konfrontation mit dem höchsten deutschen Gericht. Im Mittelpunkt der Konferenz stand die Frage, wie Datenschutz im 21. Jahrhundert gesichert werden kann. In der Erklärung heißt es unter anderem:
„Die Regelungen insbesondere zum Großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Erst das BVerfG hat mit einer Reihe grundlegender Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen. Deshalb forderte die Konferenz von der Politik eine neue Datenschutzkultur dahingehend ein, die grundgesetzlich gezogenen Grenzen nicht bis zur letzten Konsequenz auszureizen oder sogar zu überschreiten."

Meine Presseerklärung vom 08.04.2008 unter: www.lfd.niedersachsen.de Pfad: Allgemein > Aktuelles > Presseinformationen > 2008

2010:
Bundesverfassungsgericht erklärt deutsche Regelungen für verfassungswidrig

Wie zu erwarten, wurde das Bundesverfassungsgericht (BVerfG) mehrfach angerufen. Anders als sonst üblich hielten jedoch nicht nur Einzelkläger, wie der ehemalige Bundesinnenminister Gerhart Baum und der ehemalige Vizepräsident des Deutschen Bundestages, Burkhard Hirsch[8], sowie Vertreter von Bürgerrechtsbewegungen diese gesetzliche Regelung für verfassungswidrig. Beim BVerfG wurden auch Klagen von einem Verfahrensbevollmächtigten im Namen vieler Bundestagsabgeordneter der Fraktion Bündnis 90/Die Grünen[9], von der Gewerkschaft ver.di[10] sowie von weit mehr als 30.000 Klägerinnen und Klägern[11] eingereicht – ein beispielloses Massenverfahren in der deutschen Rechtsgeschichte.
Das BVerfG gab den Datenschutzbeauftragten des Bundes und der Länder Gelegenheit zur Äußerung im Verfassungsbeschwerdeverfahren. Im Wege der Abstimmung wurde am 24. Januar 2007 eine umfangreiche gemeinsame Stellungnahme verfasst. Die darin vorgetragenen Argumente mit der kritischen Beurteilung zur Verfassungsmäßigkeit fanden sich zu erheblichen Teilen in der Be-

8 Verfassungsklage Az. 1 BvR 263/08
9 Verfassungsklage Az. 1 BvR 586/08 und 2 BvE 1/08
10 Verfassungsklage Az. 1 BvR 1571/08
11 Verfassungsklage Az. 1 BvR 256/08 und 1 BvR 508/08

gründung des Urteils wieder. Der BfDI hat 2008 und 2009 in seiner Zuständigkeit als Aufsichtsbehörde über Telekommunikationsunternehmen darüber hinaus drei eigene Stellungnahmen gegenüber dem BVerfG abgegeben.[12]

Nach der mündlichen Verhandlung in Karlsruhe am 15.12.2009, an der mehrere Datenschutzbeauftragte und auch der zuständige Teamleiter meiner Geschäftsstelle teilgenommen hatten, entschied das BVerfG mit seinem Urteil vom 2.3.2010[13] einmal mehr im Sinne der Stärkung des Rechts auf informationelle Selbstbestimmung als Bestandteil des Persönlichkeitsrechtes. Die Entscheidung lautet im Tenor, dass die Regelungen der §§ 113 a Abs. 1, 113 b Satz 1 Telekommunikationsgesetz (TKG) sowie § 100 g Strafprozessordnung (StPO), soweit danach Verkehrsdaten nach § 113 a des Telekommunikationsgesetzes erhoben werden dürfen, einen Verstoß gegen das Telekommunikationsgeheimnis gemäß Art. 10 Abs. 1 Grundgesetz (GG) darstellten. Das BVerfG erklärte die Vorschriften nicht nur für verfassungswidrig, sondern für nichtig und ordnete die unverzügliche Löschung der bereits gespeicherten Vorratsdaten an. Damit verhängte das Gericht die schärfste ihm zur Verfügung stehende Sanktion gegen einen verfassungswidrigen Rechtsakt des Gesetzgebers. Das BVerfG hat zwar eine Vorratsspeicherung von TK-Verkehrsdaten nicht grundsätzlich vollständig verneint, es hat aber die verfassungsrechtlichen Grenzen aufgezeigt, die nicht überschritten werden dürfen. Das Gericht bewertet dabei inhaltlich die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt und die das Grundgesetz nicht zulässt.

Das Urteil ließ für kurze Zeit Zufriedenheit angesichts dieser erneuten Stärkung des Datenschutzes aufkommen. Danach aber brach ein neuer inhaltlicher Disput zwischen CDU/CSU und FDP über eine Neuregelung aus. Besonders Innenpolitiker befürworten nach wie vor eine Neuregelung mit einer Speicherung der Daten für sechs Monate auch ohne konkreten Anfangsverdacht, unterstützt durch die Konferenz der Innenminister (IMK) und zahlreiche Leiter von Polizeibehörden, die bisweilen auch eine Ausreizung der Obergrenze zur Speicherdauer befürworten oder diese sogar für zu kurz halten. Seitens der FDP reichen die Stellungnahmen inzwischen von der Speicherung nur in konkreten Verdachtsfällen und nachträglich per Quick-Freeze-Verfahren bis zur Totalablehnung von Datensammlungen.

Der Erfolg bei der Verfolgung von Straftaten im Internet hängt nicht davon ab, dass nur eindimensional dieses eine Instrument der Massendatenauswertung möglich ist.

Es ist in den Diskussionen fortwährend zu beobachten, dass die Seite der Befürworter einer Neuauflage der Vorratsdatenspeicherung die Emotionalität des Themas innere Sicherheit nutzt. Angst ist aber ein schlechter Berater, wenn es auch darum geht, nicht das Grundrechts-Kind mit dem Kriminalitätsbekämpfungs-Bade auszuschütten. Es gilt hier besonders, die Prinzipien Geeignetheit, Erforderlichkeit und Angemessenheit von Eingriffsnormen zu prüfen. Das kommt jedoch noch zu kurz.

Die Befürworter der Vorratsdatenspeicherung führen gerne an, dass diese ein „unverzichtbares Element der Verbrechensbekämpfung“ sei, dass ohne eine maximale Ausreizung einer Regelung eine wirksame Strafverfolgung im Internet unmöglich sei, und sie bemühen die Vokabel der nach dem Urteil entstandenen Sicherheitslücke. Dabei bleibt außer acht, dass der Erfolg bei der Verfolgung von Straftaten im Internet nicht nur von diesem einen Instrument der Massendatenauswertung abhängt. Vielmehr kommt es darauf an, dass individuell die beste Kombination verschiedener Ermittlungsmaß-

12 Stellungnahmen des BfDI gegenüber dem BVerfG
– vom 31.10.2008
http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/StellungnahmeVorratsdaten311008.html?nn=409870
– vom 10.06.2009
http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/StellungnahmeVorratsdaten100609.html?nn=409870 und
– vom 24.11.2009
http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/StellungnahmeVorratsdaten241109.html?nn=409870

13 Urteil des BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html (1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08)

nahmen zum Einsatz kommen sollte. Dabei müssen viele der einzelnen Maßnahmen nicht einmal Grundrechtseingriffe darstellen. Auch sind Zweifel an der Wirksamkeit und Geeignetheit angebracht, sofern sich die Speicherung und Nutzung der Daten gerade auf Terroristen oder organisierte kriminelle Strukturen beziehen soll. Die Speicherung kann von Tätern auf zahlreiche Arten umgangen werden, was besonders von professionellen Straftätern anzunehmen ist, indem sie etwa fremde Mobiltelefone, Internetcafés oder Telefonzellen nutzen. Damit schrumpft die Zahl der Fälle, in denen die Vorratsdatenspeicherung hilfreich wäre, erheblich.

2010: DSB-Frühjahrskonferenz ruft zu Neubewertung auf

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nahm nach dem Urteil des BVerfG im März 2010 mit der Entschließung „Keine Vorratsdatenspeicherung!“ erneut Stellung. Zur Begründung wurde darauf hingewiesen, dass die Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermögliche. Daher lehne die DSB-Konferenz die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehöre zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren sei. Die Konferenz forderte deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen. Da das BVerfG betone, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden dürfe, strahle die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und müsse auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Der Gesetzgeber sei bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

BVerfG: Die Freiheitswahrnehmung der Bürgerinnen und Bürger darf nicht total erfasst und registriert werden.

2011: BMJ legt umstrittenes Eckpunktepapier vor

Das Bundesjustizministerium (BMJ) hat im Januar 2011 ein „Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“[14] vorgelegt. Der Vorschlag zielt in insgesamt 19 Einzelpunkten auf eine grundrechtsschonendere Alternative in Form des Quick-Freeze-Verfahrens. Hier läge eine anlassbezogene Speicherungspflicht und die Sicherung relevanter Daten („Einfrierung“) vor. Diese könnte in einer zweiten Stufe mit Zustimmung eines Richters (Richtervorbehalt) den Strafverfolgungsbehörden für den zeitlich begrenzten Zugriff zur Verfügung gestellt („aufgetaut“) werden. Bei diesem Verfahren würde nur die Speicherung von bereits vorhandenen Verkehrsdaten derjenigen Personen angeordnet werden, die einen hinreichenden Anlass dazu gegeben haben.
Für die Verfolgung von Straftaten im Internet erfolgt nach diesem Vorschlag eine eng auf sieben Tage befristete Speicherung von Verkehrsdaten zu dem Zweck, bei einem konkreten Verdacht eine

14 Bundesjustizministerium: „Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet“, Stand 17.01.2011 (http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/eckpunktepapr_zur_sicherung_vorhandener_verkehrsdaten.pdf?__blob=publicationFile)

Zuordnung dynamischer IP-Adressen zu Personen, insbesondere zur Bekämpfung von Kinderpornografie im Internet, zu ermöglichen.

Während die Innenminister und die Ermittlungsbehörden diesen Kompromissvorschlag weitestgehend als ungeeignet und nicht weitgehend genug ablehnen, muss m. E. konstatiert werden, dass bereits dieses Modell eine weitergehende Einschränkung der Grundrechte beinhaltet, als dies vor der EU-Richtlinie der Fall war.

BMJ-„Eckpunktepapier zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet": www.bmj.de/DE/Buerger/digitaleWelt/QuickFreeze/quickfreeze_node.html

Am 9.6.2011 hat das BMJ einen auf diesem Modell basierenden Gesetzentwurf[15] in die Ressortabstimmung gegeben. Bei den Innenministern erhielt dieser Gesetzentwurf erneut wenig Unterstützung. Nach der Sitzung der Innenministerkonferenz (IMK) am 22.6.2011[16] demonstrierten die Teilnehmer Einigkeit darin, dass sich die Sicherheitsgesetze überwiegend bewährt hätten und dass eine schnelle Einigung bei der Neufassung des Terrorismusbekämpfungsgesetzes sowie die Schaffung einer gesetzlichen Grundlage für eine „Mindestspeicherfrist" für Verbindungsdaten zu befürworten sei. Ohne Mindestspeicherfrist sei es vom Zufall abhängig, welche Daten die Provider noch gespeichert haben. Dies sei eine gravierende Sicherheitslücke, die schnellstmöglich zu schließen sei, erklärte der IMK-Vorsitzende.

Wissenschaftlicher Dienst des Bundestages hat Bedenken

Der Wissenschaftliche Dienst (WD) des Bundestages[17] legte in einer Ausarbeitung vom 25.2.2011 „Zur Vereinbarkeit der Richtlinie über die Vorratsspeicherung von Daten mit der Europäischen Grundrechtecharta" dar, dass er Bedenken zur Möglichkeit der grundrechtskonformen Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung sehe. Er stützt sich dabei auf das Verhältnismäßigkeitsprinzip und zweifelt, ob die Angemessenheit der Regelung unter dem Gesichtspunkt der Zweck-/Mittel-Relation erfüllt sei. Der WD folgert, dass vorbehaltlich der noch ausstehenden Bewertung der Kommission, die vermutlich tragfähige Daten über die Erfolgsaussichten der Vorratsspeicherung enthalten wird, die Regelung in ihrer momentanen Ausgestaltung unangemessen in das Gemeinschaftsgrundrecht der berufs- und wirtschaftlichen Betätigungsfreiheit zu Lasten der Telekommunikationsanbieter eingreifen könnte. Der WD schließt mit Blick auf den derzeitigen Diskussionsstand zur Richtlinie 2006/24/EG und zur Auslegung der Grundrechtecharta sowie der bestehenden Umsetzungsspielräume der Mitgliedstaaten, dass zweifelsfrei keine Ausgestaltung dieser Richtlinie möglich sei, die eine Vereinbarkeit mit der Grundrechtecharta sicherstelle. Insbesondere könne nicht abschließend beurteilt werden, ob weniger eingriffsintensive Formen der Datenerhebung gegenüber der in der RL 2006/24/EG vorgesehenen anlasslosen Datenspeicherung in gleicher Weise geeignet seien, die mit dieser Richtlinie verfolgten Ziele zu verwirklichen.

---

15 „Gesetz zur Sicherung vorhandener Verkehrsdaten und Gewährleistung von Bestandsdatenauskünften im Internet", Stand 07.06.2011, http://www.computerundrecht.de/DiskE_.pdf

16 Pressemitteilung vom 22.06.2011 zur Frühjahrssitzung der Ständige Konferenz der Innenminister und -senatoren der Länder (IMK), 21.–22.06.2011 in Frankfurt am Main, http://www.hmdis.hessen.de zu TOP 18 „Auswirkungen des Urteils des Bundesverfassungsgerichts vom 02.03.2010 zu Mindestspeicherfristen (Umsetzung der Richtlinie 2006/24/EG)"
(s. auch http://www.bundesrat.de/cln_179/nn_8780/DE/gremien-konf/fachministerkonf/imk/Sitzungen/11-06-22-termin.html?__nnn=true)

17 Website des Wissenschaftlichen Dienstes des Bundestages www.bundestag.de/dokumente/wissenschaftliche-dienste/

EU-Kommission: Speicherung ist wertvolles Instrument

Auch die Europäische Kommission ist seit dem Urteil aus Karlsruhe an der Evaluierung interessiert, wie EU-Innenkommissarin Cecilia Malmström im März 2010 erklärte. Bis Jahresende werde das Gesetz unter den Gesichtspunkten der Angemessenheit, der Effektivität und der Kosten sowie der Vereinbarkeit mit der Grundrechtecharta des Lissabon-Vertrags überprüft. Der Evaluationsbericht zur Richtlinie wurde – u. a. gestützt auf eine Konsultation 2009[18] – schließlich am 18.4.2011 vorgelegt.[19] Im Ergebnis hält er an der Vorratsdatenspeicherung als „ein wertvolles Instrument für die Strafjustizsysteme und die Strafverfolgung in der EU" fest, kündigt aber Änderungsvorschläge an. Die Zahl der „Anfragen nach gespeicherten Verkehrsdaten" betrug laut Bericht im Jahre 2008 in Deutschland 12.684 Fälle. Die Zahl der Anfragen, auf die keine Daten übermittelt werden konnten – sofern übermittelt – belief sich auf 931. Da nur 9 von 27 Staaten Zahlen angeliefert haben, ist nicht von einer Aussagefähigkeit der Erhebungen auszugehen. Das bemängelte auch der Europäische Datenschutzbeauftragte Peter Hustinx,[20] und auch der Kommissionsbericht räumt ein: „Zuverlässige quantitative und qualitative Daten sind für den Nachweis der Notwendigkeit und des Wertes von Sicherheitsmaßnahmen wie der Vorratsdatenspeicherung unerlässlich. [...] Dieses Ziel konnte bislang nicht erfüllt werden."

Die Befragung der Mitgliedsstaaten bezog sich auch lediglich darauf, in welchen Fällen die Vorratsdatenspeicherung nützlich gewesen war. Es fehlt dagegen die Erhebung, in welchen Fällen die Vorratsdatenspeicherung für die Identifizierung und Ergreifung der Straftäter tatsächlich notwendig gewesen war. Der Bericht hat nach meiner Auffassung bisher insgesamt nicht hinreichend darlegen können, dass die tiefgehenden Eingriffe in die Grundrechte gerechtfertigt wären, weil die Ermittlungsmethoden auf der Grundlage dieser Datensammlungs- und -nutzungsbefugnis alternativlos und unumgänglich seien und damit gegenüber dem Interesse des Grundrechtsschutzes überwiegen würden.

Charta der Grundrechte der Europäischen Union (2007/C 303/01) unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:DE:PDF

Zu begrüßen ist, dass die Kommission im Interesse des Datenschutzes u. a. über eine kürzere Speicherdauer, Konkretisierungen im Bereich der Anforderungen an die Datennutzung sowie Präzisierungen bei den verbindlichen Regelungen zur Datensicherheit und zum Datenschutz nachdenken will. Auch die Aussage, das Quick-Freeze-Verfahren noch einmal genauer betrachten zu wollen, lässt den Schluss zu, dass bei Methodik und Datenumfang noch neue Wege beschritten werden könnten. Der Wissenschaftliche Dienst des Bundestages hatte immerhin, wie Anfang April 2011 bekannt wurde, nach einer Prüfung keine Beweise dafür gefunden, dass eine verdachtsunabhängige Protokollierung von Nutzerspuren den Ermittlern nachweisbar bei ihrer Arbeit hilft. Nach der Sachstandsanalyse des WD im Auftrag der FDP[21] gab es „in den meisten Ländern in den Jahren 2005 bis 2010 keine signifikanten Änderungen der Aufklärungsquote", und die Rate der Täterermittlung sei ein „wichtiger Indikator des Strafverfolgungssystems".

18 Konsultationsergebnisse der EU-Kommission http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm

19 „Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG)" vom 18.04.2011 http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_de.pdf und http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/484&format=HTML&aged=0&language=DE&guiLanguage=en

20 Opinion of the European Data Protection Supervisor 31.05.2011 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf

21 Meldung im virtuellen Datenschutzbüro http://www.datenschutz.de/news/detail/?nid=4871

Strengere Regelung nicht ausgeschlossen

Es fehlt die Erhebung, in welchen Fällen die Vorratsdatenspeicherung für die Identifizierung und Ergreifung der Straftäter tatsächlich notwendig gewesen war.

Auch die EU-Innenkommissarin räumte in der Erklärung zum Bewertungsbericht ein, dass „wir einen verhältnismäßigeren, einheitlicheren Ansatz für die gesamte EU brauchen". Die Kommission werde eine strengere Regelung für die Speicherung, Abfrage und Verwendung der Daten ins Auge fassen. Die Kommission führt momentan weitere Konsultationen durch und hat bereits angekündigt, sie werde „in Anbetracht dieser Bewertung eine Überarbeitung des derzeitigen Rechtsrahmens für die Vorratsdatenspeicherung vorschlagen. Sie wird in Abstimmung mit den Strafverfolgungsbehörden, der Justiz, Wirtschafts- und Verbraucherverbänden, Datenschutzbehörden und Organisationen der Zivilgesellschaft eine Reihe von Optionen erarbeiten.

Ungeachtet der Entscheidung des BVerfG und der zuvor beschriebenen grundlegenden verfassungsrechtlichen Bedenken hat EU-Justizkommissarin Viviane Reding die Umsetzung der Richtlinie in der Bundesrepublik Deutschland angemahnt. Am 16.6.2011 wurde als erste Stufe des Vertragsverletzungsverfahrens eine Stellungnahme des Bundesjustizministeriums angefordert. Bei Nichtumsetzung droht der Fortgang in Form des Vertragsverletzungsverfahrens unter Verhängung eines Zwangsgeldes gemäß Artikel 260 des Vertrags über die Arbeitsweise der Europäischen Union.

EuGH überprüft Richtlinie

Derzeit ist weiter unklar, wie in Deutschland eine rechtliche Umsetzung Bestand haben würde, denn es bleibt auch abzuwarten, wie die inhaltliche Überprüfung der EU-Richtlinie durch den EuGH im Zusammenhang mit der später in Kraft getretenen EU-Grundrechtecharta ausgeht. Das Verfahren ist auf der Grundlage eines vom irischen High Court angekündigten Vorlageverfahrens anhängig. Derzeit wird in der Innen- und Sicherheitspolitik erneut über die Notwendigkeit einer gesetzgeberischen Initiative debattiert, weil dem Anschlag in Oslo am 22.7.2011 sofort der Ruf nach neuen Sicherheitsgesetzen folgte. Dabei müssen aber – trotz des tragischen Ereignisses und seines Ausmaßes – meines Erachtens weiterhin die Argumente der Grundrechtsschranken beachtet werden, wie sie schon im Karlsruher Urteil vom 2.3.2010 für die Gesetzgebung dargelegt wurden. Auch die TK-Verkehrsdaten des Täters hätten bei der Gefahrenabwehr in diesem Fall keinen Durchbruch erzielt, weil die Tatplanung augenscheinlich völlig unbemerkt blieb.

Neue Rundfunkfinanzierung schafft neue Datenschutzrisiken

Die Finanzierung des öffentlich-rechtlichen Rundfunks stand bis Ende 2010 in der öffentlichen Diskussion. Die Änderungen durch den 15. Rundfunkänderungsstaatsvertrag (15. RÄStV) sollen am 1.1.2013 in Kraft treten, sofern in allen Bundesländern bis spätestens 31.12.2011 eine Ratifizierung, also eine parlamentarische Verabschiedung eines Umsetzungsgesetzes erfolgt ist. Ich gehe davon aus, dass auch nach dem Inkrafttreten des 15. RÄStV die bisherige Kontroverse zu den aufgeworfenen Datenschutzfragen nicht verebben wird. Im Gegenteil: Die Anwendung der wohnungsbezogenen Beitragsfinanzierung (je Haushalt und Betriebsstätte) wird neue Datenschutzbeschwerden provozieren, mindestens hinsichtlich der Erhebung und Nutzung von personenbezogenen Daten von Wohnungseigentümern, -besitzern, -mietern und Mitbewohnern in Wohngemeinschaften.

Um letzte Schwarzseher und Schwarzhörer aufzuspüren, so der ursprüngliche Plan, sollten nach den Wünschen der Rundfunkanstalten diese und die Gebühreneinzugszentrale (GEZ) über ein beispielloses Abrufverfahren aus allen möglichen öffentlichen Registern in die Persönlichkeitsrechte der gesamten erwachsenen Bevölkerung eingreifen dürfen, obwohl mehr als 95 Prozent der Haushalte ihre Fernseh- und Radiogeräte pflichtgemäß bei der GEZ angemeldet haben. So sollte die GEZ umfangreiche Befugnisse bekommen, personenbezogene Daten aus zahlreichen Registern jederzeit ohne Anlass online abrufen zu können. Die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten sollte um Übermittlungsbefugnisse aus weiteren staatlichen Dateien wie den Registern aller berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Wären diese Pläne Realität geworden, entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen, obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist. Die Vorstellungen hätten dem Verhältnismäßigkeitsprinzip eklatant widersprochen und wären daher nicht akzeptabel.

Insbesondere im Jahre 2010, in der Phase des Entwurfes zum 15. RÄStV, bei dem es um einen vollständigen Systemwechsel ging, war eine intensive inhaltliche Erörterung der Datenschutzfragen erforderlich. Eine erste schriftliche Stellungnahme der Datenschutzbeauftragten (DSB) der Länder wurde am 23. April 2010 den Staats- und Senatskanzleien zur Verfügung gestellt. Den Rundfunkreferenten der Staats- und Senatskanzleien wurden die Bedenken von anwesenden Landesdatenschutzbeauftragten zudem im April 2010 dezidiert vorgetragen, jedoch nur in Teilen inhaltlich aufgegriffen. So entstand im Mai 2010 ein Referenzmodell und ein Eckpunktepapier zur Vorlage bei der Konferenz der Regierungschefs der Länder am 10. Juni 2010 in Berlin.

Dem für Rundfunkrecht zuständigen Referatsleiter der Niedersächsischen Staatskanzlei stellte ich am 8.7.2010 erneut die Grundprobleme der Gesetzesplanungen dar, die auch schriftlich festgehalten wurden. Auf der Grundlage eines Neuentwurfs zum Staatsvertrag vom 17.8.2010 wurde zur Tagung der Rundfunkreferenten der

Fünfzehnter Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge (Fünfzehnter Rundfunkänderungsstaatsvertrag) unter: www.rlp.de/ministerpraesident/staatskanzlei/medien/

Derzeit gültiger Rundfunkstaatsvertrag unter: www.nds-voris.de/jportal/portal/t/1n10/page/bsvorisprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=181&fromdoctodoc=yes&doc.id=jlr-RdFunkStVtrNDrahmen%3Ajuris-lr00&doc.part=X&doc.price=0.0&doc.hl=1#focuspoint

Entwurf eines Gesetzes zum Fünfzehnten Rundfunkänderungsstaatsvertrag der Nds. Landesregierung vom 09.03.2011 unter: www.landtag-niedersachsen.de/Drucksachen/Drucksachen_16_5000/3001-3500/16-3437.pdf

Länder am 7.9.2010 in Hannover je eine Abordnung der Landesdatenschutzbeauftragten und der Datenschutzbeauftragten der Rundfunkanstalten eingeladen. Insbesondere zwischen dem von den Rundfunkanstalten beauftragten Gutachter, Prof. Dr. Hans Peter Bull, und den Landesdatenschutzbeauftragten konnte in wichtigen Grundsatzfragen keine Übereinstimmung erzielt werden, insbesondere nicht in der Bewertung, ob der Grundsatz der Datensparsamkeit in den Neuregelungen hinreichend Beachtung findet.
Die Konferenz der Regierungschefs der Länder nahm den Staatsvertragsentwurf im Oktober 2010 in neuer Fassung zur Kenntnis und veranlasste im Spätherbst die Vorunterrichtungen der Landesparlamente. Mit Schreiben vom 9.11.2010 stellte ich im Wege der gesetzlichen Anhörung gemäß § 22 Abs. 1 Satz 4 NDSG vorerst abschließend gegenüber der Niedersächsischen Staatskanzlei die aus meiner Sicht offenen Fragen und Problempunkte zu wichtigen Datenschutzaspekten dar. Schließlich erfolgte im Dezember 2010 die Unterzeichnung des Staatsvertrages auf der Konferenz der Regierungschefs der Länder.

Datenschutzrechtliche Bewertung wirft zahlreiche Fragen auf

Die Abkehr von der gerätebezogenen Gebührenerhebung hin zum Wohnungsbezug eines Beitrages ist grundsätzlich zu begrüßen. Wie es im Begründungstext zum Staatsvertrag meines Erachtens richtig heißt, ist anders als in der Vorgängerregelung somit „eine Nachschau hinter der Wohnungstür nicht mehr erforderlich“. Die wenig geliebte Situation, dass der Rundfunkgebührenbeauftragte an der Haustür klingelt, erübrigt sich künftig.
Das neue Modell wirft gleichwohl aus Sicht der Datenschutzbeauftragten der Länder zahlreiche Grundsatz- und Einzelfragen auf, die ich auch gegenüber der Niedersächsischen Staatskanzlei dargelegt habe:

Bewertung von Grundsatzfragen

1. Das Ziel einer deutlich datenschutzgerechteren Beitragserhebung droht auch die unterzeichnete Vertragsfassung zu verfehlen. Die Umstellung auf eine wohnungsbezogene Abgabe wird zwar wahrscheinlich zu einer geringeren Zahl zu speichernder Beitragszahler führen. Jedoch wird dies geschehen, ohne dass die Datenverarbeitungsbefugnisse der für den Einzug der Finanzmittel zuständigen öffentlich-rechtlichen Rundfunkanstalten nach dem Grundsatz der Erforderlichkeit entsprechend beschränkt werden.
2. Eine Verlagerung des Gebühren- bzw. Beitragseinzuges auf die Finanzverwaltung wäre erstrebenswert gewesen, ist jedoch von den Regierungschefs frühzeitig und grundsätzlich verworfen worden.
3. Die IT-Verfahren der GEZ haben bisher bereits eine der größten zentralen Datenbanken in Deutschland mit weit über 40 Mio. Datensätzen zur Grundlage. Die künftige „im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebenen Stelle der öffentlich-rechtlichen Landesrundfunkanstalten“ wird diese Rolle übernehmen. Sie wird angesichts eines weiteren Anwachsens des Datenvolumens aus zusätzlichen Quellen die Brisanz dieser umfangreichen zentralen Datenbank für die Bürgerinnen und Bürger weiter steigern.
4. Aus datenschutzrechtlicher Sicht widersprechen die Datenverarbeitungsbefugnisse des Staatsvertrages den Grundsätzen der Verhältnismäßigkeit, der Datensparsamkeit und Transparenz so-

wie dem verfassungsrechtlichen und rechtsstaatlichen Gebot der Normenklarheit. Die Ermächtigungen der Rundfunkanstalten und ihrer Hilfsorgane sind zu umfangreich ausgestaltet worden. Es entsteht der Eindruck, dass nach Ansicht der Verfasser des Änderungsstaatsvertrages auch in Zukunft zusätzliche umfangreiche Datenerhebungsbefugnisse für den Gebühreneinzug benötigt werden, um für jede Wohnung einen zahlungswilligen Beitragsschuldner zu finden. Diese Forderung ist jedoch unberechtigt, weil es bereits eine Anmeldepflicht gibt – oftmals sogar mehrerer beitragspflichtiger volljähriger Gesamtschuldner.

Der Teufel steckt im Detail: Bewertung von Einzeltatbeständen

1. Unzulässig: Datenerhebung bei privaten Quellen

Die Ermächtigung des § 11 Absatz 4 ermöglicht es, die für die Beitragserhebung notwendigen Daten ohne Kenntnis des Betroffenen nicht nur aus öffentlichen, sondern zusätzlich auch aus nicht-öffentlichen Quellen zu erheben. Entschärft wird dies nur durch § 14 Abs. 10, der hierzu ein befristetes Verbot bis zum 31.12.2014 ausspricht. Diese Ermächtigung bricht gleichwohl mit dem fundamentalen Prinzip, dass Daten grundsätzlich beim Betroffenen zu erheben sind. Eine Abweichung von diesem Grundprinzip wäre nur bei zwingender Notwendigkeit akzeptabel. Dies ist hier jedoch nicht der Fall. Es wurde bisher nicht dargelegt, welchen zusätzlichen Erkenntnisgewinn die Nutzung nicht-öffentlicher Datenquellen gegenüber einer ausschließlichen Nutzung der öffentlichen Quellen erbringen soll.

Diese Ermächtigung bricht mit dem fundamentalen Prinzip, dass Daten grundsätzlich beim Betroffenen zu erheben sind.

Jeder Beitragspflichtige unterliegt bereits nach § 8 Abs. 1 einer Anzeige-/Anmeldepflicht. Wenn der Meldepflicht nicht nachgekommen wird, besteht meiner Auffassung nach über die Meldebehörde oder die Datenerhebung beim Grundbuchamt als einer öffentlichen Stelle die Möglichkeit, den Eigentümer einer Liegenschaft und über dessen Auskunftspflicht die Nutzer der jeweiligen Wohnung oder Betriebsstelle zu ermitteln. Ich sehe daher keinen Grund, warum darüber hinaus auch bei nicht-öffentlichen Stellen Daten erhoben werden sollen.

Die Art der zu nutzenden nicht-öffentlichen Quellen ist nicht konkretisiert, nur die Art der Daten. Es könnten somit alle denkbaren Möglichkeiten wie etwa Arbeitgeber, Versicherungen, Versandhäuser, Inkassounternehmen und Auskunfteien in Betracht kommen. Über diese Ermächtigung soll auch zukünftig die Möglichkeit bestehen, Adressdaten aus privaten Quellen anzukaufen, was sich mit dieser Deutlichkeit beim Lesen des Regelungstextes für den Beitragsschuldner nicht unmittelbar ergibt. Gerade der Ankauf von Adressdaten bei privaten Stellen, also bei Adresshändlern, ist aber nach einer Umstellung von der Geräteabgabe auf eine Wohnungsabgabe nicht mehr erforderlich. Hinzu kommt, dass hier keine Möglichkeit für die Rundfunkanstalt besteht, die Qualität der nicht-öffentlichen Datenquelle zu überprüfen, und somit ein erhebliches Risiko besteht, dass hier mit falschen Daten gearbeitet wird (veralteten, gefälschten Daten oder falschen Dubletten, immer also Daten, deren Integrität gebrochen sein kann). Diese Erfahrung hat sich in der Vergangenheit immer wieder gezeigt. Außerdem stellt der Ankauf von großen Mengen von Adressdaten bei Dritten auch keine zielgerichtete Form der Datenerhebung dar. Es werden Daten also auf Vorrat erhoben, die ohne konkreten Verdacht auf mögliche, noch unbekannte Wohnungsinhaber überprüft werden sollen. Unter diesen Gesichtspunkten stellt sich die Befugnis der Rundfunkanstalten, die Datenerhebung beim Betroffenen oder öffentlichen Stellen zusätzlich auch auf private Quellen auszuweiten, nach meiner Rechtsauffassung als unzulässig dar.

Es besteht ein erhebliches Risiko, dass hier mit falschen Daten gearbeitet wird.

Hinsichtlich der Möglichkeit der Datenerhebung bei öffentlichen Stellen war eine Begrenzung zu fordern, die mit § 11 Abs. 4 Satz 3 im Staatsvertrag auch moderat nachgebessert wurde: Die Erhebung, Verarbeitung oder Nutzung bei den Meldebehörden muss sich nun auf die in § 14 Abs. 9 Nr. 1 bis 8 genannten Daten beschränken. Der Staatsvertrag sieht aber weiterhin eine Löschungsfrist von zwölf Monaten für die erlangten, nicht überprüften (früher: „nicht benötigten") Daten vor (jetzt § 11 Abs. 5 Satz 3, im Entwurf vom 21.10.2010 noch in § 11 Abs. 4 Satz 2). Die Löschung wird also gesetzlich erzwungen, wenn die Bearbeitung nicht innerhalb dieses Zeitraumes erfolgt. Die Erforderlichkeit einer derart langen Speicherdauer ist weiterhin nicht ersichtlich, weil davon auszugehen ist, dass ein Zuwarten von zwölf Monaten ab Erhebung dem Anspruch der schnellstmöglichen Berichtigung von personenbezogenen Daten widerspricht und im Ergebnis zu einer unangemessen langen Zwischenspeicherung führt.

Die Erforderlichkeit einer zwölfmonatigen Speicherdauer ist nicht ersichtlich.

Der Staatsvertrag lässt eine systematische nach der Eingriffstiefe abgestufte Klarstellung vermissen, dass die Daten ausschließlich beim Betroffenen zu erheben sind und nur in begründeten Ausnahmefällen ein Rückgriff auf weitere öffentliche Quellen zulässig ist. Diese Bestimmung des Gesetzesinhalts darf aufgrund der Eingriffstiefe insbesondere nicht einer Satzung im Rahmen der Satzungsermächtigung gemäß § 9 Abs. 2 überlassen bleiben, sondern ist im Staatsvertrag/Gesetz zu regeln. Es hätte außerdem sichergestellt werden müssen, dass spezialgesetzliche Erhebungs- und Verarbeitungsbefugnisse durch die Rechtfertigungstatbestände des Staatsvertrages nicht umgangen werden. Mit § 11 Abs. 4 wird ein Paralleltatbestand zur Erhebung von Daten aus öffentlichen Registern geschaffen. Die dafür erlassenen bereichsspezifischen Übermittlungstatbestände können so ausgehebelt werden. Die Landesrundfunkanstalten haben z. B. die Wahl, entweder über die melderechtlichen Vorschriften auf das Melderegister zuzugreifen oder § 11 Abs. 4 als Rechtsgrundlage heran zu ziehen. Den bereichsspezifischen Vorschriften ist hier der Vorrang einzuräumen, da sie inhaltlich bestimmt und normenklar sind.

2. Unzulässig: Scannen von Gesundheits- und Sozialdaten

Die Änderung des Staatsvertrages sieht vor, dass sich Bürgerinnen und Bürger beim Vorliegen von besonderen Voraussetzungen gemäß § 4 von der Beitragspflicht befreien lassen können oder einen Anspruch auf Ermäßigung des Rundfunkbeitrages haben. Die Befreiungstatbestände sind überwiegend im sozialen Bereich begründet. Eine Befreiung oder Ermäßigung wird auf Antrag bei Nachweis der Voraussetzungen gewährt. Nach den neuen Regelungen wären die Rundfunkanstalten berechtigt, sich zum Nachweis der Berechtigung eine Bescheinigung oder die Originalbescheide bzw. beglaubigte Kopien dieser Bescheide vorlegen zu lassen und diese zu speichern. Der Änderungsstaatsvertrag orientiert sich dabei ausschließlich an praktischen Belangen der Rundfunkanstalten, wonach die gesamte Eingangspost bei der „im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebenen Stelle der öffentlich-rechtlichen Landesrundfunkanstalten" (bislang „Gebühreneinzugszentrale", GEZ) eingescannt wird. Nur deshalb erfolgt eine vollständige Erfassung der Bescheide. Nach eigenen Aussagen der GEZ ist bei dieser Verfahrensweise eine partielle Löschung nicht benötigter Daten nicht möglich. Allein deshalb werden auch sensitive Gesundheits- und/oder Sozialdaten gespeichert, die für die Entscheidung über eine Beitragsbefreiung nicht erforderlich sind. Im übrigen ist selbst die GEZ nach Aussage von Vertretern der Landesrundfunkanstalten nicht an der damit entstehenden Datenmenge interessiert, wohl aber an einer Reduzierung auf das Wesentliche.

Die Verarbeitung nicht erforderlicher Daten widerspricht jedenfalls den Grundsätzen unserer Datenschutzrechtsordnung, insbesondere dem Grundsatz der Datensparsamkeit, der über Art. 6

Absatz 1 Ziffer c der Europäischen Datenschutzrichtlinie[1] Eingang in unsere Rechtsordnung gefunden hat. Auch das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung[2] die Geltung des weithin im Datenschutzrecht verankerten Grundsatzes der Datensparsamkeit zum Ausdruck gebracht. Dieser Grundsatz durchzieht nicht nur das Bundesdatenschutzgesetz (BDSG), sondern auch zahlreiche weitere Landes- und spezielle Gesetze über den Datenschutz. Datenschutzgerecht – weil datensparsamer – wäre es hier, die Nachweispflicht auf die Vorlage von Leistungsbescheinigungen zu beschränken, die lediglich den Leistungsgrund und den Leistungszeitraum erkennen lassen. Vielfach stellt die Leistungsverwaltung deshalb speziell so genannte Drittbescheinigungen aus. Daher sollte eine geänderte Regelung vorsehen, dass grundsätzlich Drittbescheinigungen vorzulegen sind, die dann gescannt werden könnten. Die Vorlage sollte auch auf die Fälle beschränkt sein, bei denen die Beschaffung einer Drittbescheinigung nicht möglich ist, die Vorlage des Leistungsbescheids im Original oder in beglaubigter Kopie verlangt werden kann, der dann von den Rundfunkanstalten bzw. deren Auftragsdatenverarbeiter nicht gescannt werden darf, sondern aus dem die entscheidungserheblichen Daten durch manuelle Dateneingabe gespeichert werden und der Bescheid anschließend zurückgesendet wird. Da mit einer hohen Zahl von Befreiungsanträgen aufgrund der gesamtschuldnerischen Haftung aller volljährigen Wohnungsinhaber zu rechnen ist, dürfte der nicht erforderliche Datenbestand durch den Modellwechsel mit hoher Wahrscheinlichkeit noch anwachsen.

Die Verarbeitung nicht erforderlicher Daten widerspricht den Grundsätzen unserer Datenschutzrechtsordnung.

Europäische Datenschutzrichtlinie unter:
www.lfd.niedersachsen.de
Pfad: Home > Recht > Europäisches Recht

Ein weiterer Befreiungstatbestand (§ 4 Absatz 6) soll nach der Staatsvertragsänderung in so genannten Härtefällen vorliegen. Welche konkreten Nachweispflichten hier bestehen, ist dem Vertragstext nicht zu entnehmen. Es ist jedoch anzunehmen, dass hier neben der Übermittlung von Gesundheits- und/oder Sozialdaten auch die Offenlegung von Finanz- und Steuerdaten erforderlich ist. In jedem Falle ist hier eine gesetzliche Konkretisierung des Datenerhebungsumfangs notwendig, um bei den Beitragsschuldnern die erforderliche Rechtsklarheit zu schaffen. Diesbezügliche Erläuterungen im Begründungstext zum Staatsvertrag oder zum jeweiligen Umsetzungsgesetz des Landes sind nicht ausreichend.

3. Unzulässig: Funktionsübertragung auf private Dritte

Gemäß § 10 Absatz 7 Satz 1 bedienen sich die Rundfunkanstalten bei der Beitreibung des Rundfunkbeitrages einer „im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene(n) Stelle". Mit dieser Beschreibung ist die heutige GEZ gemeint. Diese Stelle verarbeitet die erforderlichen Daten für die Beitragserhebung. Datenschutzrechtlich ist das Verhältnis zwischen den Rundfunkanstalten und der genannten Stelle als ‚Datenverarbeitung im Auftrag' zu betrachten. Einzige Aufgabe dieser Stelle ist es, die Rundfunkbeiträge von den Bürgern einzuziehen und den Rundfunkanstalten bereitzustellen. Vor diesem Hintergrund war es nicht nachvollziehbar, dass in § 10 Absatz 7 Satz 2 die Landesrundfunkanstalten außerdem ermächtigt werden sollten, diese Aufgabe zusätzlich „ganz oder teilweise" auf Dritte zu übertragen. Dies würde zu einer weiteren Datenverarbeitung durch Dritte führen und wäre nicht notwendig, es sei denn, die von den Rundfunkanstalten betriebene gemeinsame Stelle wäre nicht in der Lage, die Aufgabe zu erfüllen, die ihre Existenzberechtigung ausmacht.

Gegenüber dem Vertragsentwurf mit Stand August 2010 wurde aufgrund des nachdrücklichen Hinweises der Datenschutzbeauftragten in der letzten Fassung vom Oktober vor der

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt der Europäischen Gemeinschaften (Nr. L 281 vom 23. November 1995 S. 0031 – 0050)

2 BVerfG, 1 BvR 256/08 vom 11.3.2008, Absatz-Nr. (1 – 188), Rn. 270 http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html

Unterzeichnung auf die Formulierung einer „ganz oder teilweisen" Übertragung verzichtet. Eine vollständige Übertragung von Aufgaben auf Dritte (Wortlaut: „ganz") hätte andernfalls eine unzulässige Funktionsübertragung dargestellt. Gleichwohl sehe ich weiterhin das Problem, dass bei der neuen Formulierung eine unzulässige Funktionsübertragung zustande kommen könnte. Die Neuregelung lautet: „Die Landesrundfunkanstalt ist ermächtigt, einzelne Tätigkeiten bei der Durchführung des Beitragseinzugs und der Ermittlung von Beitragsschuldnern auf Dritte zu übertragen und das Nähere durch die Satzung nach § 9 Abs. 2 zu regeln." Zwar fehlt nun die Ermächtigung zur explizit vollständigen Übertragung, es bleibt jedoch unklar, welche Dimension eine „einzelne Tätigkeit" haben darf. Auch hier darf die Definition des Ausmaßes nicht der Satzung überlassen bleiben, sondern ist normenklar im Staatsvertragstext zu regeln.

4. Klares Verbot fehlt: Alle Rundfunkanstalten könnten auf alle Daten zugreifen

Zur Erfüllung Ihrer Aufgaben hält die im Rahmen einer nichtrechtsfähigen öffentlich-rechtlichen Verwaltungsgemeinschaft betriebene Stelle die kompletten Datensätze aller beitragspflichtigen Bürger der gesamten Bundesrepublik vor. Eine logische Trennung dieses Registers nach Zugehörigkeit zu einer bestimmten Landesrundfunkanstalt erfolgt nach dem Wortlaut des Vertragstextes nicht. Umgekehrt könnten die einzelnen Landesrundfunkanstalten Zugriff auf den kompletten Datensatz aller Beitragsschuldner der Bundesrepublik erhalten. Hinweise in der Begründung zum Vertragsentwurf oder zum Landesgesetzentwurf, dass eine strikte Trennung erfolge, reichen nach meiner Ansicht nicht aus.

Bereits in anderen Rechtsbereichen wurde die Existenz solcher bundesweiten zentralen Register als unzulässig kritisiert. Unabhängig von der grundsätzlichen datenschutzrechtlichen Kritik an solchen zentralen Datensammlungen ist hier mit dem neuen Modell der Rundfunkfinanzierung auch kein Bedarf für einen bundesweiten Zugriff auf alle Rundfunkbeitragsschuldnerdaten erkennbar. Wurde beim jetzigen Finanzierungsmodell noch an eine Person angeknüpft, die ein Empfangsgerät bereithält, ist zukünftig eine Wohnung oder Betriebsstätte Anknüpfungspunkt für die Zahlungspflicht. Da diese in der Regel ortsfest sein werden, ist nur noch der Zugriff einer Rundfunkanstalt auf die Daten erforderlich, die sich auf Wohnungen und/oder Betriebsstätten im eigenen Sendegebiet beziehen. Jede weitere Möglichkeit der Datenverarbeitung wäre unverhältnismäßig und damit unzulässig.

5. Unzulässig, weil nicht erforderlich: Pauschale Datenübermittlung durch die Meldebehörde

Der Änderungsstaatsvertrag sieht in § 14 Absatz 9 vor, dass die Rundfunkanstalten innerhalb einer Frist von zwei Jahren ab Inkrafttreten des Staatsvertrages von allen Meldebehörden einen festgelegten Datensatz aller volljährigen Personen automatisiert übermittelt bekommen, um eine Bestands- und Ersterfassung der Beitragsschuldner zu ermöglichen. Dieses gewählte Verfahren ist mit dem Grundsatz der Datensparsamkeit nicht vereinbar, da ein Grund für eine pauschale Datenübermittlung durch die Meldebehörden aufgrund der Vermutungsregelung nach § 14 Abs. 3 des Änderungsstaatsvertrages nicht besteht. Nur in Zweifelsfällen ist eine Datenübermittlung bei konkreter Anforderung erforderlich; auf diese sollte daher die Datenübermittlungsbefugnis beschränkt werden. Auch sollte zumindest die Anzeigepflicht nach § 14 Abs. 1 des Änderungsstaatsvertrages gestrichen werden, da eine voraussetzungslose und umfassende Anzeigepflicht Privater Bedenken im Hinblick auf den Verhältnismäßigkeitsgrundsatz begegnet; Beitragsausfälle dürften aufgrund der Vermutungsregelung kaum eintreten und Streitfälle ließen sich durch konkrete Datenanforderungen bei den Meldebehörden lösen, auch existiert bereits jetzt eine Meldedatenübermittlungsermächtigung in den Landesmeldegesetzen.

Das Verfahren ist mit dem Grundsatz der Datensparsamkeit nicht vereinbar.

6. Weitere datenschutzrechtliche Problempunkte

6.1 Regelungslücke Wohnungsbegriff

Obwohl seit April 2010 von den Datenschutzbeauftragten immer wieder angesprochen, ist im Änderungsstaatsvertrag keine Klarheit in der Frage geschaffen worden, was eigentlich eine Wohnung i. S. des Staatsvertrages ist und wie die Inhaberschaft letztlich nachgewiesen werden soll. Der Vertragstext wählt hier in § 3 Absatz 1 Ziffer 1 subjektive Deutungsbegriffe wie „zum Wohnen und Schlafen geeignet", um eine Wohnung zu beschreiben. Es sind durchaus Orte denkbar, die diese Geeignetheit wohl aufweisen, aber im Allgemeinen nicht als Wohnung bezeichnet werden. An dieser Regelungslücke ändert auch die Tatsache nichts, dass der (letztlich immer unvollständige) Negativkatalog in Abs. 2 geregelt wird. Unklar bleibt, wie diese Geeignetheit festgestellt werden soll. Denkbar sind hier zwar Hausbesuche oder Besichtigungen von Beitragsbeauftragten, die aber nicht mehr gewollt sind und rechtlich nunmehr unzulässig wären.

Eine volljährige Person, die eine Wohnung selbst bewohnt, ist per Legaldefinition Inhaber (§ 2 Absatz 2 Satz 1 des Änderungsstaatsvertrages) und damit Beitragsschuldner (§ 2 Absatz 1 des Änderungsstaatsvertrages). Die Inhaberschaft einer Wohnung wird jedoch vermutet, wenn der Betreffende melderechtlich erfasst ist oder im Mietvertrag als Mieter genannt wird (§ 2 Absatz 2 Satz 2 des Änderungsstaatsvertrages). Die Rechtswirkung ist mithin dieselbe, denn die Beitragsschuldnerschaft tritt damit ungeprüft in Kraft, sofern nicht der Gegenbeweis erbracht wird. Dass Mietverträge auch in nicht schriftlicher Form existieren, oder von Personen abgeschlossen werden, die nur die Mietzahlung übernehmen, bleibt in diesem Regelungskontext unberücksichtigt. Es stellt sich die Frage, wie in diesem Fall und vor allem durch Offenbarung welcher Daten hier der positive oder auch negative Nachweis der Inhaberschaft einer Wohnung durch den Betroffenen erbracht werden kann. Es sollte daher auf die einschlägigen melderechtlichen Vorschriften Bezug genommen werden; zumindest sollten diese gesetzlichen Begriffsbestimmungen unverändert übernommen werden.

Dass Mietverträge auch in nicht schriftlicher Form existieren oder von Personen abgeschlossen werden, die nur die Mietzahlung übernehmen, bleibt unberücksichtigt.

6.2 Kollektive Haftbarmachung der Bevölkerung

Ein Strukturmangel des 15. Rundfunkänderungsstaatsvertrags in datenschutzrechtlicher Hinsicht ist die Ausweitung der künftigen Rundfunkbeitragsschuld auf alle volljährigen Personen, die in Deutschland mit einem Wohnsitz gemeldet sind bzw. ein Mietverhältnis begründet haben. Anknüpfungspunkt für die Beitragsschuld ist eine gesetzlich angeordnete Fiktion, wonach jede Person als Wohnungsinhaber gilt, die nach dem Melderecht gemeldet oder im Mietvertrag für eine Wohnung als Mieter genannt ist. Der Personenkreis, der nach dem Änderungsstaatsvertrag künftig als Wohnungsinhaber gilt, haftet den Rundfunkanstalten bzw. den Beitragsgläubigern gemäß § 2 Abs. 3 Satz 1 des Änderungsstaatsvertrages als Gesamtschuldner.

Aus der Sicht der Beitragsgläubiger stellt die Fiktion der Wohnungsinhaberschaft eine Erleichterung bei der Durchsetzung des Rundfunkbeitrags dar. Denn der Gesamtschuldner schuldet grundsätzlich die gesamte Leistung, d. h. den gesamten Rundfunkbeitrag für die Wohnung, in der er wohnt, und zwar unabhängig davon, ob er selbst Inhaber der Wohnung oder lediglich Mitbewohner ist. Dies bedeutet unter Datenschutzgesichtspunkten eine Ausdehnung des Kreises von möglichen Beitragsschuldnern auf Personen, die, ohne einen eigenen Haushalt zu führen, künftig legitimes Subjekt des Datenerhebungsinteresses der Beitragsgläubiger werden können. Statt eine Lösung zu wählen, die die Rechtspflichten an die tatsächliche Wohnungsinhaberschaft nur eines Haushaltsvorstands knüpft, arbeitet das Regelungskonzept mit einer großen Streubreite, bei der eine kollektive Haftbarmachung der Bevölkerung die Verantwortlichkeit auf die Betroffenen selbst verlagert. Insofern wäre ein grundlegendes Umsteuern des Änderungsstaatsvertrages in dem Sinne, dass nur eine Person pro Haushalt Beitragsschuldner ist, mehr als nur wünschenswert gewesen. Nach dem Modell, wie es mit dem Änderungsstaatsvertrag nun vorliegt, müsste jedoch, besonders bei den Löschungsvorschriften, klarer

Nur eine Person pro Haushalt als Beitragsschuldner wäre mehr als nur wünschenswert gewesen.

zwischen Beitragsschuldnern und Beitragszahlern unterschieden werden, damit deutlich wird, dass die Daten aller übrigen in einer Wohnung gemeldeten und im Mietvertrag genannten Personen gelöscht werden, wenn ein Beitragszahler ermittelt wurde.

6.3 Unzulässig: Wer sich befreien will, muss Daten anderer liefern

An unterschiedlichen Stellen werden im Änderungsstaatsvertrag den Beitragsschuldnern für verschiedene Sachverhalte pauschal Nachweispflichten auferlegt. So hat ein Beitragsschuldner, der einen Antrag auf Befreiung von der Beitragspflicht stellt, gemäß § 4 Absatz 7 Satz 3 des Änderungsstaatsvertrages in diesem Antrag nicht nur die weiteren volljährigen Bewohner seiner Wohnung zu benennen, sondern hat dies (gemeint ist wohl deren Existenz und die Tatsache, dass diese auch Bewohner der Wohnung sind) auch nachzuweisen. Diese Pflicht betrifft jeden Antragsteller, unabhängig davon, ob er die Wohnungsabgabe bezahlen will oder aber nur im Innenverhältnis als Gesamtschuldner einen Nachweis benötigt, dass er nicht zahlen muss. Im Vertragstext ist zudem nicht erkennbar, in welchem Umfang diese Nachweispflicht besteht. Es stellt sich die Frage, wie weit der Betroffene hier gezwungen ist, im Einzelfall Daten Dritter zu erheben und an die Rundfunkanstalt zu übermitteln, um seiner Nachweispflicht zu genügen. Die Regelung verletzt den Grundsatz der Datenerhebung beim Betroffenen. Sie birgt die konkrete Gefahr in sich, dass persönliche, darunter ggf. auch sensitive Daten Dritter, gegen deren Willen den Rundfunkanstalten offenbart werden. Nach meiner Auffassung wird dieses Problem besonders am Beispiel von Wohngemeinschaften deutlich.

6.4 Unzulässig: Nachweispflicht bei Betriebsstilllegung ohne Gesetz

In § 5 Absatz 4 (früher Absatz 5) des Änderungsstaatsvertrages wird einem Betriebsstätteninhaber eine Befreiung vom Rundfunkbeitrag gewährt, wenn er glaubhaft macht und auf Verlangen nachweist, dass seine Betriebsstätte für mehr als drei Monate stillgelegt wird. Auch hier ist nicht erkennbar, welchen Umfang die Nachweispflicht hat. Aufgrund der Unklarheit ist anzunehmen, dass hier im Einzelfall auch gesundheitliche, familiäre oder sonstige private Tatsachen belegt werden müssen. Eine solche erzwungene Offenlegung stellt regelmäßig einen erheblichen Grundrechtseingriff dar. Zwar wird für die Konkretisierung durch Satzung, die auf der Satzungsermächtigung in § 9 Absatz 2 des Änderungsstaatsvertrages fußt, hingewiesen, dies kann jedoch zur Schaffung von Rechtsklarheit nicht ausreichen. Erhebliche grundrechtsrelevante Eingriffe müssen im Gesetz selbst, also durch die Legislative, geregelt werden. Hier diese Befugnis auf die Exekutive zu delegieren, entspricht nicht den verfassungsrechtlichen Anforderungen an den Grundsatz des Gesetzesvorbehaltes.

6.5 Unzulässig: Rundfunkanstalten wollen Begründung für Auszug

Warum sollten die Rundfunkanstalten daran interessiert sein, zu erfahren, aus welchen in seiner Person liegenden Gründen ein Beitragsschuldner die Abmeldung vornimmt?

In § 8 Absatz 5 Ziffer 2 (vormals 3) des Änderungsstaatsvertrages wird von einem Beitragsschuldner, der pflichtgemäß das Ende des Innehabens einer Wohnung oder Betriebsstätte anzeigt (Abmeldung) gefordert, dass er den „die Abmeldung begründenden Sachverhalt“ mitteilt. Für den Abmeldevorgang allein würde die Mitteilung, dass eine Wohnung oder Betriebsstätte verlassen oder aufgegeben wird, ausreichen. Nicht nachvollziehbar ist, warum die Rundfunkanstalten daran interessiert sein sollten, zu erfahren, aus welchen in seiner Person liegenden Gründen ein Beitragsschuldner die Abmeldung vornimmt. Der Betroffene könnte nach der Formulierung im Staatsvertrag gezwungen werden, Gesundheits-, Sozial-, Finanz- und/oder Steuerdaten zu offenbaren und ggf. familiäre Verhältnisse offen zu legen. Auch die in § 8 Abs. 5 Nr. 3 des Änderungsstaatsvertrages vorgesehene Datenerhebung über Dritte beim (bisherigen) Beitragsschuldner be-

gegnet Bedenken. Personenbezogene Daten sind nach dem Grundsatz der Direkterhebung grundsätzlich beim Betroffenen selbst zu erheben. Ausnahmen hiervon können zwar durch Gesetz angeordnet werden, setzen aber die strikte Beachtung des Verhältnismäßigkeitsgrundsatzes voraus. Inwieweit hier die Datenerhebung bei einem Dritten erforderlich ist, erschließt sich nicht, da nach § 8 Abs. 1 des Änderungsstaatsvertrages der neue Beitragsschuldner selbst zur Meldung verpflichtet ist und von ihm auch nach § 9 Absatz 1 des Änderungsstaatsvertrages Auskunft begehrt werden kann.

6.6 Zu unbestimmt: Erhebung „weiterer Daten"

Nach § 9 Abs. 1 Satz 4 des Änderungsstaatsvertrages soll die zuständige Landesrundfunkanstalt im Einzelfall weitere Daten, die über die Daten nach § 8 Abs. 4 und 5 hinausgehen, bei Eigentümern und Verwaltern erheben dürfen, soweit dies nach Satz 1 erforderlich ist. Der Begriff „weitere Daten" ist ein unbestimmter Rechtsbegriff, der im Staatsvertrag schon deswegen zu konkretisieren ist, da nach § 9 Abs. 1 Satz 6 auch insoweit Zwangsbefugnisse eröffnet werden sollen. Für den Auskunftspflichtigen muss klar erkennbar sein, wie weit seine Auskunftspflicht tatsächlich geht. Erforderlich ist in den Fällen, in denen der Beitragsschuldner unbekannt ist, allein die Benennung des Wohnungs- oder Betriebsstätteninhabers und damit eines möglichen Beitragsschuldners. Alle weiteren Angaben haben die Landesrundfunkanstalten dann bei den Betroffenen selbst zu erheben.

6.7 Bedenklich: Löschungsfristen zu lang

Der Änderungsstaatsvertrag geht davon aus, dass nicht benötigte Daten zu löschen sind. Dies ist grundsätzlich richtig. Der Vertrag legt hierfür jedoch eine Frist von zwölf Monaten fest, so in § 11 Absatz 5 Satz 3. Das Erheben, Speichern oder das anderweitige Verarbeiten von personenbezogenen Daten, die für die Aufgabenerfüllung nicht benötigt werden, ist durch öffentliche Stellen grundsätzlich unzulässig. Nicht erforderliche Daten sind daher unverzüglich oder innerhalb einer kurz zu bemessenden Frist zu löschen. Diesem Grundsatz folgend dürfte diese Bestimmung rechtswidrig sein.

7. Gesetzgeber muss für Normenklarheit sorgen

Die Hoffnung, dass diese vorgenannten Probleme im Rahmen einer Nachbesserung zum Änderungsstaatsvertrag noch ausgeräumt werden, wurde bis Ende 2010 im Wesentlichen nicht erfüllt.

Die angekündigte Begründung zum Änderungsstaatsvertrag ist mir erst mit der Fassung vom 15.02.2011 bekannt geworden. Allerdings sind Mängel in der Normenklarheit und fehlende Bestimmtheit von Ermächtigungen und Pflichten im Wortlaut einer Rechtsnorm ohnedies nicht durch Ausführungen der Begründung, wie in der Landtagsdrucksache 16/3437 veröffentlicht, kompensierbar. Ich hatte auch Zweifel an der Zulässigkeit, dass einigen Regelungen erst nach Unterzeichnung des Staatsvertrages durch die Regierungschefs eine inhaltliche Bedeutung gegeben werden sollte.

Auch der Weg, eine Bereinigung und Klärung durch die Rechtsprechung abzuwarten, wie dies bereits verschiedentlich in Gesprächen zu vernehmen war, ist nach meiner Auffassung nicht zielführend. Zwar ist die Rechtsprechung auch für die Ausfüllung unbestimmter Rechtsbegriffe in strittigen Fällen zuständig, sie sollte jedoch nicht bereits im Rechtsetzungsprozess als Regulativ einkalkuliert werden. Ich kann keinen Hinderungsgrund erkennen, dass der Gesetzgeber bereits für Normenklarheit und Bestimmtheit sorgen kann.

Niedersachsen: Änderungsanträge abgelehnt, Gesetz beschlossen

Im weiteren parlamentarischen Fortgang auf Landesebene habe ich auf Einladung des Ausschusses für Bundes- und Europaangelegenheiten und Medien (AfBuEuM) des Niedersächsischen Landtages diesen in seiner Sitzung am 1.4.2011 über meine Einschätzung umfassend unterrichtet und darauf hingewiesen, dass ich eine Nachbesserung des Gesetzentwurfs zum Staatsvertrag für erforderlich halte, um den Grundsätzen der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit gerecht zu werden. Andernfalls könnte nach meiner Auffassung nicht ausgeschlossen werden, dass in der praktischen Umsetzung der Regelungen schwerwiegende Spannungen – nicht nur von Seiten der Wirtschaft – zu erwarten seien.
In seiner Sitzung am 13. Mai 2011 empfahl der AfBuEuM nach abschließender Beratung dem Plenum des Landtages – vorbehaltlich der Zustimmung des mitberatenden Ausschusses für Rechts und Verfassungsfragen – mit den Stimmen der Fraktionen der CDU, der SPD und der GRÜNEN, bei Stimmenthaltung der Fraktion der LINKEN, dem Gesetzentwurf zum Fünfzehnten Rundfunkänderungsstaatsvertrag zuzustimmen. Ein Änderungsantrag der Landtagsfraktion Bündnis 90/Die Grünen[3] („15. Rundfunkänderungsstaatsvertrag – Erhebung des Rundfunkbeitrags datensparsam gestalten") fand im Ausschuss keine Mehrheit. Er empfahl dem Landtag mit den Stimmen der Fraktionen der CDU und der SPD und gegen die Stimmen der Fraktionen der GRÜNEN und der LINKEN, den Gesetzentwurf abzulehnen. Die von mir vorgetragenen Bedenken fanden im Ergebnis ebenfalls keinen Niederschlag. Offenbar galt es, den bereits unterzeichneten Vertrag der Länder nicht zu blockieren, da die Zustimmung aller Länder für das Inkrafttreten erforderlich ist.
Der Niedersächsische Landtag hat schließlich in seiner Sitzung am 28.6.2011 das Gesetz mehrheitlich verabschiedet und anderslautende Änderungsanträge abgelehnt.[4] Die datenschutzrechtlichen Einschätzungen waren hier im wesentlichen nicht mehr inhaltlicher Beratungsgegenstand.

3 Antrag der Fraktion Bündnis 90/Die Grünen - Drs. 16/3015, http://www.landtag-niedersachsen.de/Drucksachen/Drucksachen_16_5000/3001-3500/16-3015.pdf
4 108. Sitzung des Nds. Landtages am 28.06.2011, Tagesordnungspunkt 5, Plenarprotokoll: http://www.landtag-niedersachsen.de/infothek/steno/steno_16_WP/2011/endber108.pdf

Privatsphäre unverschlüsselt: Funk-Überwachungskameras oft ohne Mindestschutz

Funk-Überwachungskameras sind inzwischen für wenig Geld erhältlich. Da ist es für Kleingewerbetreibende oder auch Privatpersonen verlockend, im Interesse der vermeintlichen Sicherheit zuzugreifen und ohne umfangreiche Kabelverlegung Geräte zur Überwachung und Aufzeichnung zu installieren. Was technisch wenig spektakulär erscheint, ist datenschutzrechtlich ein häufig unterschätztes Problem, weil rechtliche Anforderungen oft unbekannt sind und Schutzmaßnahmen völlig fehlen.

Durch Berichte in den Medien kam zu diesen Geräten im Berichtszeitraum erneut die Frage nach der Sicherheit auf. Was journalistisch als neues Thema schien, war aus rechtlicher wie technischer Sicht fachlich bereits lange bekannt. Gleichwohl wurde deutlich, dass hier die Öffentlichkeit verstärkt informiert werden muss über die gebotene Datensparsamkeit, einen deutlich sensibleren Umgang mit Videoüberwachungstechnik sowie die rechtlichen Rahmenbedingungen. Außerdem sind Hersteller und Handel aufgerufen, die Produkte nach dem Prinzip „Privacy by Design“ bereits datenschutzfreundlich zu entwickeln und auf den Markt zu bringen.

Was ist anders als bei „Profianlagen“?

Als klein, leistungsstark und preiswert werden sie beworben, und tatsächlich bieten die im Elektrohandel frei verkäuflichen Funk-Überwachungsanlagen Beachtliches: Für bereits unter 100 Euro sind mittlerweile Kamerasets erhältlich, die mit einer Reichweite von bis zu 100 m drahtlose Videoüberwachungen ermöglichen.
Die Einsatzmöglichkeiten sind vielfältig, doch nicht alle erfolgen im Rahmen einer rechtlich zulässigen Verwendung. Während das Beobachten von Sachen in der Regel keiner weiteren datenschutzrechtlichen Überlegung bedarf, sind jedoch Persönlichkeitsrechte zu beachten, sobald Menschen in den Beobachtungsbereich treten oder das Beobachten von Sachen personenbeziehbare Lebensumstände betrifft. Stark miniaturisierte und batteriebetriebene Kameras sowie die problemlose Übertragung und Aufzeichnung von qualitativ hochwertigem Bild- und Tonmaterial könnten auch zu bewusst missbräuchlicher und illegaler Nutzung verführen.
Ungeachtet der rechtlichen Problematik, auf die in den meisten Produktbeschreibungen und Bedienungsanleitungen nur unzureichend oder gar nicht hingewiesen wird, ergibt sich allerdings auch ein technisches Problem: Die Funkübertragung erfolgt in der Regel unverschlüsselt in dem frei zugänglichen Frequenzbereich von 2,4 GHz, der beispielsweise auch von Bluetooth- und WLAN-Geräten (WLAN = Wireless Local Network, drahtlose lokale Netzwerke) zur drahtlosen Kommunikation genutzt wird. Somit ist jede in Sendereichweite befindliche Empfangsstation technisch in der Lage, die Funksignale zu empfangen und offene oder sogar heimliche Beobachtungen und Aufzeichnungen zu ermöglichen. Die Rechtmäßigkeit des Erhebens, der Übertragung und des Empfangens solcher Videobilder ist jedoch durchaus nicht immer gegeben.
In der Verantwortung steht hier in erster Linie der Betreiber der Funkkamera, also derjenige, der sie mit einem bestimmten Zweck installiert hat oder hat installieren lassen. Werden mit seinem Gerät rechtmäßig personenbezogene Daten erhoben (Bilderfassung), verarbeitet und übertragen (etwa an ein Empfangsgerät, einen Monitor, einen Webserver oder ein Aufzeichnungsgerät), steht er in der Pflicht, diese gegen möglichen Missbrauch (unbefugter Zugriff und Weitergabe) hinreichend abzusichern.

Angesichts der Sensitivität dieser Daten bietet eine unverschlüsselte Übertragung nicht genug Schutz für die Vertraulichkeit und Integrität der Daten und Informationen. Es ist vielmehr ein dem Stand der Technik entsprechendes Verschlüsselungsverfahren zu verwenden. Auf § 9 Bundesdatenschutzgesetz (BDSG) und insbesondere die Nr. 3 (Zugriffskontrolle) und Nr. 4 (Weitergabekontrolle) der Anlage zu § 9 BDSG bzw. nach § 7 Niedersächsisches Datenschutzgesetz (NDSG) wird ausdrücklich hingewiesen. Ohne Verschlüsselung der gesendeten Daten wären nicht befugte Personen zum Empfang der Videos in der Lage. Für diesen rechtswidrigen Zustand ist der Betreiber verantwortlich; allerdings handelt natürlich auch der Angreifer rechtswidrig.
Die hierin liegende Problematik zum technischen und organisatorischen Datenschutz wird in vergleichbarer Weise auch in der Orientierungshilfe „Datenschutz in drahtlosen Netzen" aufgegriffen, die der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet hat.

Datenschutzrechtliche Mindestanforderungen:

- Bevor eine drahtlose Videoübertragung in Erwägung gezogen wird, sollte zunächst immer der alternative Einsatz von kabelgebundener Übertragung geprüft werden.
- Die Hersteller und der Einzelhandel von Videoüberwachungsanlagen müssen den Kunden gegenüber umfassend Informationen und Fachberatung anbieten, einschließlich der rechtlichen Einsatzbeschränkungen, der Schutzmaßnahmen wie Verschlüsselung, Authentisierungsmechanismen usw..
- Käufer müssen sich ihrer Verantwortung und der Unzulänglichkeit bestimmter Produkte bewusst werden und im Zweifel ein technisch abgesichertes Produkt wählen.
- Betreiber dieser Videoanlagen müssen die erforderlichen technischen und organisatorischen Maßnahmen nach § 7 NDSG bzw. § 9 BDSG treffen.
- Vor dem Einsatz solcher Geräte sind grundsätzlich eine Vorabkontrolle und gegebenenfalls ein Datenschutzkonzept erforderlich.
- Die besonderen datenschutzrechtlichen Vorschriften nach § 25 a NDSG (Beobachtung durch Bildübertragung) und § 6b BDSG (Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen) sind zu beachten.

Strafrechtliche Bedeutung bei Funk-Überwachungskameras

Dass mit fehlerhafter Handhabung von Video- und Tonaufnahmen und Übertragungen sehr leicht gegen das Strafrecht verstoßen werden kann, wird durch die folgenden Szenarien deutlich. Diese sind jedoch keinesfalls als abschließende Aufzählung zu verstehen.

- **Wardriving**
  Nach § 89 i. V. m. § 148 Abs. 1 Nr. 1 Telekommunikationsgesetz (TKG) ist unerlaubtes Abhören einer Funkanlage eine Straftat. Wardriving, also das unbefugte Nutzen eines offenen WLANs, könnte im Einzelfall als solche gewertet werden. Die Rechtsprechung ist hier aber bisher leider nicht einheitlich. Ein „Camdriving" auf 2,4 GHz-Netze ist ein ähnlicher Vorgang wie das Wardriving als Angriff auf WLAN-Netze und daher rechtlich vergleichbar.
- **Sprachaufzeichnungen**
  § 201 Strafgesetzbuch (StGB) Verletzung der Vertraulichkeit des Wortes
  „Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt
  1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
  2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht."

„Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt."

- **Bildaufnahmen**
  § 201 a StGB Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen
  „Wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt oder überträgt und dadurch deren höchstpersönlichen Lebensbereich verletzt, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."
  Ebenso ist der Gebrauch und die Zugänglichmachung dieser Aufnahmen strafbar.
  Unter Umständen könnte auch für den Betreiber der Videoanlage ein Unterlassungstatbestand nach § 13 StGB erfüllt sein, sofern er durch Unterlassen von Schutzmaßnahmen den Datenmissbrauch ermöglicht.
- **Ausspähen und Abfangen von Daten**
  Weiteres strafrechtlich relevantes Verhalten würde sich auch in folgenden Fällen ergeben:
  – § 202 a StGB Ausspähen von Daten (unter Überwindung der Zugangssicherung)
  – § 202 b StGB Abfangen von Daten (unter Anwendung von technischen Mitteln)
  – § 202 c StGB Vorbereiten des Ausspähens und Abfangens von Daten

Informationen des BfDI unter: www.bfdi.bund.de/cln_134/SharedDocs/Publikationen/Arbeitshilfen/Schutzprofil.html

Datenschutzgerechte Videosoftware

Neben der Problematik der Datenübertragung sind jedoch eine Reihe weiterer Aspekte zu beachten. Beispielsweise sind Anforderungen an die Software zur Verarbeitung von personenbezogenen Bilddaten zu stellen. Diese sind definiert in einem Schutzprofil, das vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik herausgegeben wurde (Common Criteria Protection Profile, BSI-PP-0023, Version 2.0, vom 15.01.2007).

Common Criteria Protection Profile: Software zur Verarbeitung von personenbezogenen Bilddaten. Dieses auf den Common Criteria basierende Schutzprofil (Protection Profile – PP) thematisiert die Mindestanforderungen, die an die Software zur Verarbeitung von personenbezogenen Bilddaten gestellt werden, um einerseits den datenschutzrechtlichen Bestimmungen zu genügen und andererseits eine anwenderfreundliche Bedienung der IT-Sicherheit moderner Videoüberwachungsanlagen zu ermöglichen.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Home > Technik und Organisation > Vorabkontrolle
Themenseite Videoüberwachung und Datenschutz
Pfad: Home > Themen/Stichworte > Videoüberwachung
Datenschutz in drahtlosen Netzen
Pfad: Home > Technik und Organisation > Netzwerke > Drahtlose Netze

ID-Management in der Landesverwaltung: Ohne Schutzmaßnahmen droht Gefahr

Die technische Umsetzung der Europäischen Dienstleistungsrichtlinie nimmt der Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) zum Anlass, die Einführung eines zentralen Identitätsmanagements (ID-Management) für die Anwendungen der niedersächsischen Landesverwaltung exemplarisch zu erproben. Unter einem ID-Management wird allgemein ein Verfahren verstanden, mit dem es möglich ist, gezielt, transparent und selbstgesteuert die Identitäten sowie im Bedarfsfall Anonymität und Pseudoanonymität zu verwalten.

Das bisherige Modell sieht vor, das ID-Management so zu gestalten, dass es mit möglichst wenig Aufwand in bestehende Anwendungen integriert werden kann. Das gewinnt insbesondere Bedeutung, wenn in IT-Anwendungen so genannte serviceorientierte Architekturen genutzt werden sollen, also die Orchestrierung von Komponenten verschiedener Herkunft über das Internet. Diese Orchestrierung konfektioniert die System- und Anwendungssoftware zu einem abgeforderten Dienst oder stellt sie völlig individuell zusammen. Dabei kommt es darauf an, die Identitätsdaten integer, konsistent, verlässlich und hochverfügbar zu verwalten, zu speichern und den berechtigten IT-Anwendungen bei Bedarf bereitzustellen.

Ein nicht sauber implementiertes ID-Management birgt Missbrauchspotential bis hin zum Identitätsdiebstahl.

Die Zusammenfassung aller Berechtigungen eines Nutzers innerhalb einer zentralen ID-Management-Anwendung ermöglicht einerseits eine umfassende und aktuelle Umsetzung aller für eine Person bestehenden Berechtigungen, birgt andererseits aber auch Gefahren und Missbrauchspotential bis hin zum Identitätsdiebstahl mit der missbräuchlichen Nutzung weitreichender Rechte. So ist das Missbrauchspotential bezüglich der Schadenshöhe eines solchen zentralen Rechte-Speichers gegenüber unabhängigen Berechtigungssystemen ungleich größer, sofern ein nicht entdeckter Softwarefehler existiert, der eine Sicherheitslücke darstellt. Ebenso verhält es sich hinsichtlich der notwendigen, sehr hohen Verfügbarkeit der zentralen ID-Management-Anwendung, denn ein Ausfall dieses Systems zieht alle abhängigen Applikationen mit in die Nichtverfügbarkeit. Andererseits bietet diese zentrale Lösung auch große Vorteile und Chancen: Ein sauber implementiertes ID-Management wäre als fehlerfreies System für alle Umgebungen verfügbar und muss nur einmal gepflegt und fortentwickelt werden. Das setzt aber auch voraus, dass beispielsweise durch ein ganzheitliches akribisch implementiertes Backup-/Restore-Management und durch ein dupliziertes System (Redundanz) die Ausfallsicherheit höchstmöglich verbessert wird. Sofern diese Gegebenheiten und Gefahren schon bei der Konzeption hinreichend berücksichtigt und in der Folge auch entsprechend durch Planung angemessener Schutzmaßnahmen umgesetzt werden, gehe ich davon aus, dass die daran anknüpfenden datenschutzrechtlichen Probleme zufriedenstellend gelöst

werden können. Ein probates Werkzeug auf diesem Weg ist eine umfassende Betrachtung der Probleme im Rahmen einer datenschutzrechtlichen Vorabkontrolle und die Darstellung der sich daraus ergebenden Maßnahmen in einem detaillierten Sicherungskonzept.
Angesichts der steigenden Komplexität von IT-Anwendungen und der Vielzahl der integrativen Entwicklungen im IT-Bereich wird es in Zukunft immer mehr Bedeutung haben, dass international anerkannte best-practice-Ansätze, Normen und Standards beachtet werden.
Bemühungen für eine internationale Normung von Identitätsmanagement und Datenschutz im Bereich der IT-Sicherheitsverfahren gibt es inzwischen auf internationaler Ebene als Arbeitsentwürfe („ISO/IEC 24760, CD“ bei der ISO/IEC JTC 1/SC 27 Working Group 5) und seit 2006 in Deutschland bei der Arbeitsgruppe NIA 27-05 des Deutschen Institut für Normung e.V. (DIN).
Besondere Bedeutung bei derartigen zentralen Systemen hat eine Strategie, bei der die technologischen Entwicklungen beobachtet und verfolgt werden, um die im Sinne des § 7 NDSG erforderliche Angemessenheit technisch-organisatorischer Maßnahmen auf dem Stand der Technik sicherzustellen und um zu verhindern, dass veraltete Ansätze implementiert werden.
Ich gehe davon aus, dass der LSKN mich auch weiterhin gemäß § 22 Absatz 2 NDSG über den Fortgang des Projekts informieren wird und meine datenschutzrechtlichen Hinweise entsprechende Berücksichtigung bei der Realisierung finden.

Weitere Informationen:

www.iso.org/iso/iso_technical_committee?commid=45306
Normenausschuss Informationstechnik und Anwendungen (NIA) unter:
www.nia.din.de

Des Kaisers neue Provider – vom Risiko, am Ende nackt dazustehen

Seit einigen Jahren finden innerhalb der Landesverwaltung im Bereich IT-Planung, -Koordination und -Administration große Umwälzungen statt. Während auch diese Aufgabengebiete ursprünglich mehr oder weniger uneingeschränkt der Ressorthoheit unterlagen, wurden im Rahmen der Verwaltungsreform Optimierungs- und Einsparpotentiale gerade auch bei den Planstellen gesehen, in Kabinettsbeschlüssen Handlungsziele vorgegeben und in der Folge zahlreiche Projekte gestartet, die vor allem der Zentralisierung, Konsolidierung, Beherrschbarkeit und Zukunftsorientierung dienen sollten. Mit ihrer Realisierung sind nicht zu unterschätzende Gefahren für den Datenschutz verbunden.

Startete das Großprojekt „mit.niedersachsen" noch unter der Ägide des Innenministeriumsreferats ZIM (Zentrales Informationsmanagement; siehe auch meinen XVIII Tätigkeitsbericht, S. 54 ff.), so wurde in der Folge die Funktion des CIO (Chief Information Officer) geschaffen, dessen Geschäftsstelle dem Niedersächsischen Ministerium für Inneres und Sport angegliedert ist. Diese Stelle wurde um einen CISO (Chief Information Security Officer) ergänzt, der die strategische Planung des Informationssicherheitsmanagements für die Landesverwaltung verantwortet. Meine hierzu immer wieder vorgetragenen datenschutzrechtlichen Forderungen (siehe auch meinen XIX Tätigkeitsbericht, S. 61) lauten:

- Klare Definition von Zuständigkeiten und Verantwortlichkeiten.
- Mehr Transparenz durch erhöhte Dokumentationspflichten.
- Schaffung eines breit angelegten, verbindlichen und überprüfbaren IT-Sicherheits- und Datenschutzmanagements.
- Realistische Bewertung der durch Zentralisierung und vermehrter Auftragsdatenverarbeitung neu entstehenden Gefährdungen mittels rechtzeitiger Risikoanalysen und Vorabkontrollen.

In meinem XIX. Tätigkeitsbericht 2007–2008 hatte ich zur Notwendigkeit eines systematischen Managements der Informationssicherheit und zu den Verzögerungen bei der Aufstellung einer IT-Sicherheitsleitlinie und IT-Sicherheitsrichtlinien bereits ausführlich Stellung bezogen.

izn erfüllte nicht alle Anforderungen

Nicht alle Zielerreichungsgrade wurden rechtzeitig und offen kommuniziert.

Als Ausfluss der unter einigem Zeitdruck erzielten Teilprojektergebnisse wurden dem Informatikzentrum Niedersachsen (izn) in großem Maße Verantwortlichkeiten für den IT-Betrieb in der Landesverwaltung übertragen, die vorher bei den Ressorts lagen. Der erhoffte Transfer von zusätzlicher Kompetenz und Stellenanteilen in Richtung Dienstleister blieb allerdings aus, und die Bemühungen des Landesbetriebes, sich geeignetes Personal am freien Markt zu beschaffen, waren aus verschie-

Vilhelm Pedersen (1820 – 1859)
Illustration zu „The Emperor's New Clothes."
Quelle: Wikipedia

denen Gründen oft erfolglos oder deckten zumindest nicht den zahlenmäßigen Bedarf. Nicht alle Zielerreichungsgrade wurden aus meiner Sicht rechtzeitig und offen kommuniziert und mancher Hinweis auf offensichtliche Probleme erfolgte nur hinter vorgehaltener Hand. Mit anderen Worten: Das dann auch noch in den Landesbetrieb für Statistik und Kommunikation (LSKN) eingegliederte izn war bei bestem Willen und allem Engagement seiner Mitarbeiter häufig nicht in der Lage, die gestellten Anforderungen in vollem Umfang zu erfüllen.

Private Sub-Provider sollen es besser machen

Was mit dem Projekt TK2010 zur Neuorientierung der Telekommunikationsnetze und -technologien für die Landesverwaltung erstmals in besonderer Größenordnung in Erscheinung trat (siehe auch meinen XIX Tätigkeitsbericht, S. 62), findet immer häufiger Anwendung. Aus insgesamt komplexen und umfangreichen IT-Strukturen werden zunehmend Arbeitsfelder herausgefiltert, die zur Übernahme durch außen stehende Auftragnehmer (sogenannte Provider) geeignet erscheinen. War der LSKN einst noch als öffentlich-rechtlicher „Allround-Provider" der Ressorts konzipiert, treten nunmehr spezialisierte privat-rechtliche „Sub-Provider" in Aktion, die nach komplexen Ausschreibungsverfahren und von stattlichen Vertragswerken geleitet an die Arbeit gehen. Neben den bereits etablierten Netz-Providern, treten Storage-Provider (für das Storage Management, also das gemanagte Massenspeicherumfeld), Desktop-Service-Provider (für den Support der Systeme und der Endgeräte am Arbeitsplatz der Bediensteten) und im Rahmen des allgegenwärtig diskutierten Cloud-Computing vielleicht bald auch noch weitere Hardware- und Software-Provider in Erscheinung. Als neueste Disziplin im Outsourcing-Geflecht wird „Provider-Management", die Kunst, alle externen Dienstleister zielführend zu koordinieren, betrieben.

Zusätzliche Risiken für den Datenschutz

In der Regel handelt es sich bei den meisten in der Landesverwaltung verarbeiteten Daten um personenbezogene oder personenbeziehbare Daten, auf die das Niedersächsischen Datenschutzgesetz (NDSG) Anwendung findet. Und die Verantwortung für deren datenschutzgerechte Verarbeitung verbleibt trotz aller Organisationsreformen und Beauftragungsverhältnisse gem. §§ 6 und 7 NDSG bei dem ursprünglichen Auftraggeber, also der öffentlichen Stelle, die ein bestimmtes Verfahren betreibt (z. B. der OFD Niedersachsen mit dem Bezügeabrechnungsverfahren KIDICAP). Damit verpflichten Organisations- und Auftragskontrolle zur Überwachung der Einhaltung sämtlicher erforderlicher technisch-organisatorischer Sicherungsmaßnahmen. Fiel dies in der Vergangenheit schon gegenüber dem LSKN schwer, verursacht jedes neue Glied in der Beauftragungskette zusätzliche Risiken und Probleme.
Auf verschiedenen Sitzungen des KA-IT (Koordinierungsausschuss-IT), nunmehr abgelöst durch den Niedersächsischen IT-Planungsrat, habe ich auf folgende, meist über die Jahre schleichend hinzukommende Gefährdungen hingewiesen:

- überhöhte Komplexität der Gesamtstrukturen,
- Verlust der Transparenz,
- Verlust des Gefühls der Verantwortlichkeit,
- Verlust des Fachwissens,
- Verlust der Kontrollmöglichkeit.
- Ursachen- und Wirkungspfeile ließen sich hier kreuz und quer ziehen.

Verbindliches Regelwerk fehlt weiterhin

Wichtig bleibt, dass man am Ende nicht ganz nackt dasteht. Die aufgezeigten Risiken beherrschbar zu gestalten bedeutet, dass neben der Realisierung möglicher Einsparpotentiale durch Outsourcing an anderer Stelle auch wieder in eigenes Personal investiert werden muss, damit Dienststellen, Ressorts und LSKN Datenschutz und Informationssicherheit inklusive IT-Sicherheit in ihrer jeweiligen zu definierenden Verantwortung qualifiziert gewährleisten können. Während in einzelnen Bereichen sehr positive Ansätze verfolgt werden, fehlt es leider noch immer an einem übergreifenden und für die ganze Landesverwaltung verbindlichen Regelwerk, das neben allgemeinen Zielsetzungen auch den Willen zur Schaffung zuständiger und verantwortlicher Strukturen erkennen lässt. Meiner bereits im XIX. Tätigkeitsbereich (siehe dort S. 61) erhobenen Forderung, dieses Regelungsvakuum zu füllen, wurde auch in den vergangenen zwei Jahren nicht gefolgt.

Ungesicherte Altpapiercontainer und wenig Geld für Verbesserungen: Zahlreiche Kommunen mit Datenschutzmängeln

Auch in den Jahren 2009 und 2010 hat mein Technik-Team wieder insgesamt zwei Gruppenprüfungen im kommunalen Bereich durchgeführt. Dabei wurden insgesamt elf Städte Gemeinden, Samtgemeinden und Flecken sowie zwei Kreisverwaltungen hinsichtlich der technisch-organisatorischen Maßnahmen überprüft. Ein Schwerpunktthema dieser Prüfungen war die Datenträgerverwaltung, wobei hierzu nicht nur Datenträger aus dem Umfeld der Informationstechnik gehören, sondern auch der Umgang mit personenbezogenen Daten auf Papier eine wichtige Rolle spielt (zur Prüfung von Bürgerbüros in Kommunen siehe Beitrag auf Seite 12).

Leider hat sich die Vermutung bestätigt, dass gerade auch scheinbar einfache Sachverhalte wie datenschutzgerechte Entsorgung von Altpapier erhebliche Probleme bereiten können. Die Spanne reicht dabei von Fehlkopien am offen zugänglichen Kopierer bis hin zu ungesicherten Altpapiercontainern am Straßenrand. Die bei Stichproben vorgefundenen Dokumente bezogen sich auf Sachverhalte aus dem Ausländer- und Sozialrecht ebenso wie auf Ausschreibungs- und Abrechnungsunterlagen der Hochbauabteilung. Dies ist umso erstaunlicher, als in den meisten Fällen geeignete technische Einrichtungen zur datenschutzgerechten Entsorgung vorhanden waren. Hier fehlt es offenbar an der notwendigen Sensibilität der Bearbeiter ebenso wie an wirksamen organisatorischen Regelungen.
Daneben hat sich bestätigt, dass die bereits in meinem letzten XIX. Tätigkeitsbericht genannten technischen und organisatorischen Mängel (siehe dort S. 73) offenbar bei den meisten Verwaltungen anzutreffen sind. Darüber hinaus haben sich weitere Gemeinsamkeiten herauskristallisiert, die ebenso auf die große Mehrzahl der Prüfungsteilnehmer zutreffen:

- Die Prüfungsgespräche vor Ort sind durch offene und konstruktive Mitarbeit gekennzeichnet und werden eher als Hilfestellung denn als Prüfung empfunden. Es gibt offenbar einen großen Bedarf nach qualifizierter Beratung, der sich aber erst konkretisiert, wenn es „ernst" wird.
- Es ist eine hohe Bereitschaft zur Beseitigung von Mängeln erkennbar, sofern dieses mit überschaubaren Kosten möglich ist. Bei der Finanzierung grundlegender technischer Maßnahmen werden im politischen Raum allerdings eher andere Prioritäten gesetzt.
- Es zeigt sich eine deutliche Untergrenze für die notwendige personelle Größe und finanzielle Leistungsfähigkeit der Verwaltungen. Zu kleine Verwaltungseinheiten sind schlichtweg nicht in der Lage, eine ordnungsgemäße Administration der eingesetzten Informations- und Kommunikationstechnik sowie die praxisgerechte Erstellung und Pflege notwendiger organisatorischer Regelungen selbst zu realisieren. Hier muss intensiv über mehr Zusammenarbeit oder die vermehrte Nutzung von datenschutzgerechter Auftragsdatenverarbeitung nachgedacht werden.

XIX.Tätigkeitsbericht: www.lfd.niedersachsen.de Pfad: Allgemein> Tätigkeitsberichte > 2007–2008

Die bei meinen Prüfungen festgestellten Mängel sollen kurzfristig abgestellt werden; die Umsetzung der erforderlichen Maßnahmen wird von mir nach einer angemessenen Frist durch Stichproben vor Ort kontrolliert. Im Ergebnis der abgeschlossenen Gruppenprüfungen hat sich erneut gezeigt, dass der eingeschlagene Weg einer Prüfung und Beratung vor Ort richtig und für beide Seiten – Kommunen und Datenschutzaufsicht – unverzichtbar ist. Der mir entstandene erhöhte Personal- und Sachaufwand ist auch durch die Übertragbarkeit der Schwerpunkt-Ergebnisse auf andere Daten verarbeitende Stellen und den Zugewinn an eigenen praktischen Erfahrungen, die sich positiv auf die übrige Beratungs- und Schulungstätigkeit auswirken, mehr als gerechtfertigt.

4

Schwerpunktthema: Videoüberwachung

Videoüberwachung durch Behörden und Kommunen: Zahlreiche Rechtsverstöße

Im Berichtszeitraum lag ein Schwerpunkt der Tätigkeit in der Überprüfung des Einsatzes von Videotechnik durch öffentliche Stellen. Schon bei ersten Erhebungen und Kontrollen vor Ort wurde deutlich, dass bei der Anwendung derartiger optisch-elektronischer Anlagen viele (rechtliche) Probleme nicht gelöst worden waren.

Bei der Landesregierung, der Polizei und Justiz erfolgte eine vollständige Erhebung. Bei sonstigen Landesbehörden und Kommunalverwaltungen waren lediglich Stichproben möglich, um einen repräsentativen Eindruck von den Anwendungsformen und deren Rechtmäßigkeit zu erlangen. Allen öffentlichen Stellen in Niedersachsen ist über § 25 a NDSG die Möglichkeit eröffnet, Videotechnik unter bestimmten Voraussetzungen einzusetzen. Darüber hinaus lassen diverse Spezialgesetze ebenfalls den Einsatz von optisch-elektronischen Systemen zu.

Keine Vorabkontrollen, keine Verfahrensbeschreibungen, Kameras auf Toiletten

Bei der Staatskanzlei und den neun Ministerien kommen ausschließlich Videoüberwachungsmaßnahmen nach § 25 a NDSG zum Einsatz. Kennzeichnungen waren unvollständig oder nicht vorhanden, Vorabkontrollen und Verfahrensbeschreibungen nicht erstellt worden. Bei drei Liegenschaften waren die Kameras in der Lage, auch so genannte Privatzonen aufzunehmen, die dem Grundrechtsschutz des Art. 13 GG unterliegen. Die Kameras der anderen ausgewählten Landesbehörden wiesen die gleichen Mängel auf. Auch hier mussten diverse Kennzeichnungspflichten nachgeholt sowie Vorabkontrollen und Verfahrenbeschreibungen nachträglich gefertigt werden.
Justizvollzugsanstalten sind in der Regel mit besonders gesicherten Hafträumen ausgestattet, in denen Häftlinge untergebracht werden, bei denen unter anderem Flucht- oder Suizidgefahr besteht. Das Niedersächsische Justizvollzugsgesetz (NJVollzG) lässt eine Beobachtung dieser Zellen lediglich zur Nachtzeit zu. Obwohl eine Erlaubnisnorm zum Einsatz von optisch-elektronischen Hilfsmitteln tagsüber nicht vorhanden ist, wurden die Zellen auch am Tage videoüberwacht. Grundsätzlich sind diese Hafträume auch mit Toiletten ausgestattet. Im Rahmen von Datenschutzkontrollen wurde festgestellt, dass die Toilettenbereiche ebenfalls mittels Videotechnik beobachtet wurden. Hierbei war zudem nicht sichergestellt, dass die Überwachungsmonitore nur durch Vollzugspersonal des gleichen Geschlechts wie die Beobachteten eingesehen wurden. Während das Justizministerium meiner Rechtsauffassung zu einer widerrechtlich Beobachtung zur Tageszeit und Aufzeichnung nicht folgen wollte, räumte man die Verletzung der Menschenwürde durch die direkte Toilettenüberwachung ein. Diese Bereiche wurden durch verschiedene Varianten (z. B. Auspixelung oder Blenden) von der Übertragung ausgeschlossen.

An einigen Gerichtsstandorten wurden Vorführzellen optisch-elektronisch überwacht. Für diese Art der Videoüberwachung ist zurzeit keine ausreichende Rechtsgrundlage vorhanden.

Die meisten Kameras im Justizvollzug werden innerhalb der Einrichtungen eingesetzt, um die Flure, Arbeits- und Freizeitbereiche zu kontrollieren. Eine ausreichende Rechtsgrundlage für diesen Videoeinsatz konnte nicht feststellt werden, so dass ich das Justizministerium aufgefordert habe, diese gesetzliche Lücke zu schließen. Das Justizministerium war hierzu allerdings nicht bereit, da es die Auffassung vertritt, die allgemeinen Datenerhebungsnormen des NJVollzG seien für den Rechtseingriff ausreichend.

Keine Rechtsgrundlage für den Videoeinsatz in den Fluren sowie den Arbeits- und Freizeitbereichen der Justizvollzugsanstalten

Keine Hinweisschilder für nicht erkennbare Kameras

Eine Polizeidirektion verwendet nach § 32 Abs. 3 NSOG an sechs Standorten Kameras, die in einer Höhe angebracht sind, die sich nicht mehr im normalen Sichtfeld der Menschen befinden. An drei weiteren Standorten werden so genannte Domkameras eingesetzt, die sehr leicht mit lichttechnischen Einrichtungen verwechselt werden können. Somit kann man nicht mehr von der gesetzlich geforderten „offenen" Überwachung sprechen. Auch eine zwischenzeitlich durchgeführte Veröffentlichung aller Kamerastandorte im Internet macht diese Art der Videoüberwachung nicht gesetzeskonform. Daher habe ich eine Kennzeichnung dieser Örtlichkeiten gefordert, zu der die zuständige Polizeidirektion nicht bereit war. Mittlerweile hatte sich auch ein Aktionsbündnis dieser Problematik angenommen und die Polizei auf Kennzeichnung vor dem Verwaltungsgericht verklagt. Nachdem das Verwaltungsgericht festgestellt hatte, dass die Kameraüberwachung der Polizeidirektion mangels Erkennbarkeit rechtswidrig sei, legte die Polizeidirektion zunächst Berufung ein. Kurz vor Ablauf der Berufungsbegründungsfrist zog sie die Berufung jedoch zurück und begann mit der Kennzeichnung der Videokameras. Der Kläger hat also in vollem Umfang obsiegt und so zu einer datenschutzgerechten Lösung beigetragen. Ob die Kennzeichnung im jeweiligen Einzelfall den gesetzlichen Anforderungen entspricht, werde ich im Rahmen meiner Kapazitäten nach und nach überprüfen.

Eine Polizeiinspektion überwachte die potentiell gefährdete Liegenschaft einer jüdischen Gemeinde. Die Kamera und das Aufzeichnungsgerät waren bei der örtlichen Berufsfeuerwehr aufgebaut. Die Kabel zwischen Kamera und Aufzeichnungsgerät waren nicht manipulationssicher verlegt, und der Videorekorder war für alle Angehörigen der Feuerwehr frei zugänglich. Die Anlage wurde nach einer Datenschutzkontrolle vor Ort vollständig abgebaut, da sie offensichtlich aus Sicht der Polizei nicht mehr erforderlich war.

Scheinsicherheit: Videoüberwachung mit defekten Geräten

Eine Stadtverwaltung stellte dem örtlichen Polizeikommissariat eine Videoüberwachungsanlage für die Bahnhofsunterführung zur Verfügung. Das Aufzeichnungsgerät fiel 2004 und die sechs Kameras fielen 2008 aus. Ein Austausch der defekten Geräte fand nicht statt. Erst nach der Datenschutzkontrolle wurde die gesamte Anlage abgebaut, die dem Bürger seit geraumer Zeit eine Scheinsicherheit vorgespiegelt hatte.

Eine andere Kommune finanzierte zwei Videokameras und ein Aufzeichnungsgerät, um der Polizei eine Überwachung einer Straßenbahnendhaltestelle zu ermöglichen. Der behördliche Datenschutzbeauftragte der Polizei kam bei der gesetzlich vorgeschriebenen Vorabkontrolle zu dem Ergebnis, dass eine Videoüberwachung mit Aufzeichnung nicht zulässig sei. Der Polizeipräsident setzte sich über diese Feststellung hinweg und veranlasste den Echtbetrieb. Auch ich kam zu dem Ergebnis, dass die festgestellte Kriminalitätslage für diese Form der Datenverarbeitung nicht ausreichend ist. Weder war die zuständige Polizeidirektion bereit, die Maßnahmen zu beenden, noch wollte der Bürgermeister das von ihm finanzierte technische Gerät zurückziehen. Bemerkenswert: Bei dieser Videoüberwachung fiel das Auszeichnungsgerät für 15 Wochen aus. Dies wurde erst bemerkt, als die Aufnahmen anlässlich einer begangenen Straftat ausgewertet werden sollten.

Polizeipräsident setzt sich über die rechtliche Beurteilung seines Datenschutzbeauftragten hinweg.

Im Rahmen von Videoaufnahmen im Zusammenhang mit versammlungsrechtlichen Aktionen wurden innerhalb einer Polizeidirektion zweimal pauschale Speicherzeiten von sechs Monaten für das angefertigte Videomaterial eingeplant. Hierbei handelte es sich um eine unverhältnismäßig lange Vorratsdatenspeicherung.

Zwei Polizeidirektionen verweigerten trotz vorhandener Rechtspflicht die Übersendung von Einsatzunterlagen, anhand derer ich die polizeilichen Videoüberwachungsmaßnahmen datenschutzrechtlich prüfen wollte.

Wesentliche Mängel in Schulen und Schwimmbädern

Der Einsatz von optisch-elektronischen Systemen bei den überprüften Kommunalverwaltungen – Landkreise, Städte und Gemeinden – erfolgt in der Regel in den Bereichen Rathäuser, Museen, Parkhäusern, Schulen, Schwimmbäder, Sozialämter und Unterführungen für Fußgänger. Neben den bekannten Problembereichen – Anbringung von Hinweisschildern, Fertigung von Vorabkontrolle und Verfahrensbeschreibung – wurden wesentliche Mängel bei Schulen und Schwimmbädern festgestellt.

Eine größere Stadt hatte vor einiger Zeit ein Verkehrsmanagement eingeführt, das u. a. mit Videotechnik an zentralen Kreuzungsbereichen ausgestattet war. Eine Überprüfung der technischen Möglichkeiten ergab, dass die Kameras mit vollständigen Schwenk- und Zoomfunktionen ohne Ausblendung von so genannten Privatzonen eingerichtet waren. Zudem war und ist eine Rechtsgrundlage für eine präventive Videoüberwachung mit Datenerhebung im Verkehrsbereich (Erkennbarkeit von Fahrzeugführern, Kfz-Kennzeichen oder Fahrzeugbeschriftungen) nicht vorhanden. Die Kameras wurden nach Aufforderung ersatzlos abgebaut.

In mehreren kommunalen Schwimmbädern mussten Kameras neu ausgerichtet werden, die teilweise oder auch vollständig in Umkleidebereiche blicken konnten. Eine Stadtverwaltung hatte von 57 Kameras 25 Attrappen in einem Parkhaus, mehreren Schulen und einer Unterführungen eingesetzt. Eine derart hohe Quote konnte in keiner anderen Kommunalverwaltung festgestellt werden. Die Attrappen wurden nach meiner Aufforderung abgebaut.

Bei der Videoüberwachung von Schulen setzte der behördliche Datenschutzbeauftragte einer Stadtverwaltung in der vorgeschriebenen Vorabkontrolle sachgerechte Maßstäbe, um Manipulationen an dem technischen Gerät zu verhindern. In der Realität jedoch wurden die Kabel ohne besondere Sicherung über eine Fassade und Flachdächer geführt. Eine Kamera wurde mit einem ausgesonderten Fahrradkorb versehen, der als vandalismussicheres Gehäuse gelten sollte.

Eine Kommunalverwaltung ließ die Vorräume ihre öffentlichen Toiletten im Rathaus mittels zweier Videokameras überwachen. Der Einsatz dieser Technik wurde als Eingriff in den höchst persönlichen Lebensbereich gewertet und untersagt.

Eine gemeinsame Videowand für Firma, Behörden und Polizei

Die Verkehrsmanagementzentrale (VMZ) Niedersachsen ist in Räumlichkeiten eines Verkehrsbetriebs untergebracht und nutzt einen gemeinsamen Lageraum, der unter anderem mit einer Videowand ausgestattet ist. An den Einzelarbeitsplätzen wirken neben den Mitarbeiterinnen und Mitarbeiter des Unternehmens auch Angehörige einer Landesbehörde, der örtlichen Kommunalverwaltungen sowie der Polizei mit. Die angeführten Organisationen betreiben eine Verbundanlage, auf die grundsätzlich ein direkter bzw. einzelfallbezogener Zugriff möglich ist. Bei der Datenschutzkontrolle konnten keine so genannten Rollen- und Berechtigungskonzepte festgestellt werden. Ausblendungen zum Schutz von Privatzonen waren nicht vorhanden, und die Schwenk- und Zoombereiche lagen außerhalb der gesetzlichen Rahmenbedingungen. Durch die offene Gestaltung des Lageraumes und die von allen einsehbare Videowand erfolgen zwischen öffentlichen und nicht-öffentlichen Stellen nahezu konstant Datenübermittlungen, die nicht gesetzeskonform sind.

Die Verkehrsmanagementzentrale Niedersachsen arbeitet zur Zeit an einem Konzept, das einen datenschutzrechtlich einwandfreien Betrieb der Kameras ermöglichen soll.

Als Serviceangebot überträgt die VMZ Niedersachsen Bilder von eigenen und fremden Kameras (u. a. der Polizei) in das Internet. Diese Variante wurde bereits im Rahmen der EXPO 2000 von mir rechtlich beurteilt und gegenüber der damaligen MOVE-Gesellschaft (heute

VMZ Niedersachsen) unter der Voraussetzung zugelassen, dass nur Übersichtsaufnahmen ohne personenbezogene oder personenbeziehbare Daten in das Internet übertragen werden. Im Rahmen der Datenschutzkontrolle wurde allerdings festgestellt, dass diese Forderung offensichtlich nicht umgesetzt worden war. Auch gezoomte Bilder mit deutlichem Personenbezug waren im Internet sichtbar. Die VMZ arbeitet zur Zeit an einem Konzept, das einen datenschutzrechtlich einwandfreien Betrieb ermöglichen soll.

Einzelkontrollen in Hannover und Delmenhorst

Offene Briefe, Berichterstattungen in den Medien und Eingaben von Privatpersonen sowie Interessengruppen machten mich auf diverse vermeintlich nicht gesetzeskonforme Anwendungsfälle von Videoüberwachung aufmerksam, die entsprechende Datenschutzkontrollen nach sich zogen. So wurden die Anlagen der Landeshauptstadt Hannover einer vollständigen Erhebung und Kontrolle unterzogen und sämtliche Installationen an den allgemeinbildenden Schulen in Delmenhorst überprüft; gleiches gilt für die Leibniz-Universität Hannover. Die Überprüfung der sonstigen Videokameras bezog sich auf einzelne Liegenschaften an Schulstandorten, auf Sportanlagen und sonstige öffentliche Gebäude. Bei diesen Kontrollen wurden immer wieder Mängel festgestellt, die sich nicht von dem Ergebnis der landesweiten Erhebung und Kontrolle unterschieden.

Gesichtsausdrücke als Hinweise auf mögliche Gefahren

Bei dem Projekt „APFel – Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme“ handelt es sich um ein bewilligtes Verbundprojekt des Bundesministeriums für Bildung und Forschung zum Thema „Mustererkennung“. Das Förderungsvolumen beträgt rund zwei Millionen Euro. Kern des Projekts ist die Ermittlung der Bewegungen von zuvor als verdächtig eingestuften Menschen. „APFel“ soll nicht nur den bisher zurückgelegten Weg der Person automatisch zeigen, sondern auch eine Vorhersage über den wahrscheinlichsten Aufenthaltsort treffen. Dies geschieht mithilfe eines speziellen Videosystems, das die Bewegungen, sogar Gesten und Gesichtsausdrücke mit typischen Mustern vergleicht und als Indiz für eine mögliche Gefahr analysiert.
Nachdem dieses Vorhaben in den Medien bekannt gemacht wurde, nahm ich dies zum Anlass, das Projekt einer datenschutzrechtlichen Würdigung zu unterziehen und die beteiligten Organisationen ausführlich zu beraten. Das Vorhaben setzt die Nutzung der unter anderem in den Publikumsbereichen von Flughäfen bereits vorhandenen Videoüberwachungsanlagen voraus und würde zu einer mit der aktuellen Rechtslage nicht vereinbaren Zweckerweiterung bzw. -änderung der Videoüberwachungstechnik führen. Die an dem Projekt Beteiligten haben daher mittlerweile davon Abstand genommen, die Testphase des APFel-Projektes in Niedersachsen fortzusetzen.

Kameraattrappen sind immer rechtswidrig

Bei dem Einsatz von Attrappen (so genannte Dummies) und dauerhaft defekten bzw. nicht genutzten Kameras findet keine Datenerhebung statt. Somit werden keine Daten verarbeitet, und das NDSG findet keine Anwendung. Diese Kameravarianten greifen zwar nicht in das Recht auf informationelle Selbstbestimmung, wohl aber in das Recht auf freie Entfaltung der Persönlichkeit

der Betroffenen ein (Artikel 2 Abs. 1 Grundgesetz), da sie zu einer Verhaltensbeeinflussung führen und auch führen sollen. Beim Bürger wird der Anschein einer Datenverarbeitung erweckt, so dass die Auswirkungen für den Betroffenen die gleichen wie bei einer „echten" Datenverarbeitung sind. Dies wird gegebenenfalls noch durch entsprechende Hinweisschilder bestärkt. Eine Rechtsgrundlage für diesen Grundrechtseingriff ist nicht vorhanden; somit ist der Einsatz dieser Varianten immer rechtswidrig.

Ergebnis der Erhebungen und Kontrollen unter:
www.lfd.niedersachsen.de
Pfad: Themen > Videoüberwachung > Kontrolle der Videoüberwachung öffentlicher Stellen 2009/2010

Enttäuschendes Gesamtergebnis

Das eher enttäuschende Gesamtergebnis der umfangreichen Erhebungen und Kontrollen habe ich am 20. April 2010 auf einer Pressekonferenz ausführlich dargestellt. Einschließlich weiterer Einzelkontrollen wurden im Berichtszeitraum 4.231 Kameras einer datenschutzrechtlichen Bewertung unterzogen, wobei 1.642 Kameras vor Ort, die restlichen Anlagen nach Aktenlage beurteilt wurden. Neben den regelmäßig wiederkehrenden Mängeln – fehlende Kennzeichnungspflicht, fehlende Vorabkontrolle, fehlende Verfahrensbeschreibung – mussten aufgrund der Überprüfungen 81 Videokameras sowie 51 Attrappen abgebaut werden. Nachträgliche Ausblendungen, Auspixelungen oder Beschränkungen der Schwenk- und Zoombereiche waren bei 215 Geräten erforderlich. In 88 Fällen wurde die Würde des Menschen verletzt. 1309 Überwachungseinrichtungen wurden ohne ausreichende Rechtsgrundlage betrieben. In einer Vielzahl von Fällen waren keine konkreten Löschfristen vorgesehen. Oftmals wurde die Speicherdauer von der Größe der Festplatte und nicht von sachlichen Erwägungen bestimmt. Auch waren Speicherzeiten von 14 Tagen bis zu drei Monaten keine Seltenheit. Zum Kontrollzeitpunkt war klar zu erkennen, dass die öffentlichen Stellen die mit verstärkter Videoüberwachung einhergehende größere Verantwortung bislang nicht ernst genommen hatten. Das Bewusstsein für Risiken und Gefahren einer Videoüberwachung war in weiten Bereichen völlig unterentwickelt.
Ich habe den Ausschuss für Inneres und Sport sowie der Unterausschuss Justizvollzug und Straffälligenhilfe des Niedersächsischen Landtages über die Ergebnisse der Prüfung ausführlich informiert. Auch mit diversen Einzelberatungen und Vorträgen in verschiedenen Gremien (z. B. Datenschutzinstitut Niedersachsen, Schulleiterkonferenz Delmenhorst, BTQ Niedersachsen GmbH) konnten Informationen zu diesem Thema breit gestreut werden.
Um den verantwortlichen Stellen für die Zukunft mehr Rechts- und Handlungssicherheit beim Einsatz von Videokameras zu geben, haben meine Mitarbeiterinnen und Mitarbeiter mehrere Orientierungshilfen (Allgemeines, Schule, Fußballspiele und sonstige Großveranstaltungen) sowie eine Musterdienstanweisung für die Kommunalverwaltung entwickelt. Sie sind auf meiner Homepage unter dem Pfad „Themen > Videoüberwachung" abrufbar.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Themen > Videoüberwachung

Videoüberwachung in der Wirtschaft nimmt seuchenartig zu

Auch im aktuellen Berichtszeitraum bildete der in allen Bereichen der Wirtschaft ungebremst fortschreitende Einsatz von Videoüberwachungsanlagen einen meiner Prüfungsschwerpunkte. So häuften sich nicht nur die Beschwerden von Bürgerinnen und Bürgern wegen der zunehmenden Zahl der Kameras in den Filialen von Lebensmittelketten oder in Einkaufscentern. Auch in Friseurgeschäften, Handyläden, Apotheken, Boutiquen, Bäckereien oder in Restaurants der Systemgastronomie breitet sich der Einsatz von Videokameras geradezu seuchenartig aus. Selbst in Arztpraxen scheinen Videoüberwachungsanlagen mittlerweile zur normalen Ausstattung zu gehören.

Dabei berufen sich die verantwortlichen Stellen zumeist auf § 6 b Abs.1 Nr. 3 BDSG. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Als Gründe für eine Videoüberwachung werden häufig generalpräventive Zwecke wie die Furcht vor Warendiebstahl, Einbruch, Sachbeschädigung und der Schutz der Beschäftigten vor tätlichen Übergriffen gewalttätiger Kunden genannt. Die Prüfungspraxis zeigt jedoch, dass sich die Geschäftsinhaber nur unzureichend darüber Gedanken machen, dass drei grundlegende Kriterien für einen zulässigen Kameraeinsatz vorliegen müssen: die Geeignetheit, die Erforderlichkeit und die Verhältnismäßigkeit. Nur wenn alle drei Kriterien erfüllt sind, ist eine Videoüberwachung datenschutzrechtlich zulässig.

Was ist bei Videoüberwachung zu beachten?

Jede Videoüberwachung ist ein Eingriff in das Persönlichkeitsrecht, denn jeder hat das Grundrecht, sich in der Öffentlichkeit unbeobachtet bewegen zu können.

Daher ist Videoüberwachung

- immer begründungsbedürftig (vor deren Beginn ist der konkrete Zweck der Überwachung schriftlich in einer Verfahrensdokumentation festzulegen und i.d.R. einer Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten zu unterziehen),
- nur als ultima ratio zulässig (vor ihrer Einrichtung müssen alle Alternativen hierzu geprüft werden),
- stets auf das nötige Maß zu beschränken und einer regelmäßigen Überprüfung der Erforderlichkeit zu unterziehen,
- stets offen durchzuführen (die Videoüberwachung muss nach außen durch geeignete Beschilderung erkennbar sein),
- planungsintensiv, kostspielig, aufwändig und nur begrenzt effektiv.

Rechtliche Anforderungen oft unbekannt

Natürlich liegt es im berechtigten Interesse des Betreibers eines Geschäftes mit hoher Kundenfrequenz, sich vor Diebstahl, Übergriffen oder Vandalismusschäden zu schützen. Allerdings ist eine Videoüberwachung nur dann ggf. erforderlich, wenn es auch tatsächlich zu solchen Vorfällen gekommen ist. Die Vorfälle sollten daher durch Vorlage einer Strafanzeige belegt werden können. Die sorgfältige Dokumentation von Vorfällen, vor denen Videoüberwachungsanlagen schützen sollen, ist aber auch geboten, um die Erforderlichkeit der Fortsetzung einer solchen Maßnahme zu präventiven oder repressiven Zwecken jederzeit darlegen zu können.

Ferner muss größeres Augenmerk darauf gerichtet werden, dass die Videoüberwachung so ausgestaltet ist, dass sie zur Erreichung der in einer Verfahrensdokumentation (§ 4 e BDSG) festzulegenden Zwecke geeignet ist. Sicherheitsgewinne lassen sich regelmäßig nur durch ein so genanntes Monitoring, also durch die lückenlose Beobachtung von Livebildern durch eingriffsbereites Personal erzielen. Erfolgt die Videoüberwachung dagegen nur in Form einer Aufzeichnung der Kamerabilder (black box-Verfahren), so sind damit keine Sicherheitsgewin-

ne verbunden. Allenfalls lassen sich dann mit den gespeicherten Bildern im Nachhinein unter Umständen Straftäter identifizieren. Schließlich hat die Prüfungspraxis ergeben, dass die mittels Videokameraeinsatz erhobenen und gespeicherten Daten häufig nicht durch entsprechende technisch-organisatorische Maßnahmen nach § 9 BDSG ausreichend geschützt werden.
All dies zeigt, dass Nutzer von Videoüberwachungsanlagen oft mit der komplexen Technik überfordert sind und dem Sachverstand von Errichterfirmen vertrauen müssen, die ihrerseits aber leider zu häufig nur in der Lage sind, solche Anlagen zu installieren, ohne auf die dabei gebotenen datenschutzrechtlichen Kenntnisse zurückgreifen zu können. In den allermeisten Fällen ist daher vor dem Einsatz von Videoüberwachungstechnik eine Vorabkontrolle durch einen betrieblichen Datenschutzbeauftragten (§ 4 d Abs. 5 und 6 i.V.m. § 4 f Abs.1 S. 6 BDSG) unverzichtbar.

Ausbreitung der Videoüberwachung hinnehmen oder gegensteuern?

Neben diesen in der Prüfungspraxis regelmäßig festzustellenden Mängeln birgt aber auch die technische Entwicklung erhebliche Risiken für die Persönlichkeitsrechte der von Videoüberwachung Betroffenen. So verleitet die mittlerweile in jedem Bau- oder Supermarkt zu einem geringen Preis erhältliche Videotechnik nicht nur viele Menschen zu deren vorschnellem und unüberlegtem Einsatz. Die Technik ermöglicht vielmehr bereits eine „intelligente Videoüberwachung“, die Gesichter erkennen und auf bestimmte auffällige Bewegungen von Zielpersonen reagieren kann. Insbesondere die Vernetzung der Kameras ist in Teilbereichen ohne Weiteres möglich.
Wir stehen also an einem Scheideweg: Entweder werden wir die unkontrollierte und unkontrollierbare Ausbreitung der Videoüberwachung mit ihrem fortschreitenden Potential einer lückenlosen Analyse auch des Verbraucherverhaltens hinnehmen und unser Privatleben und Verhalten weiter einschränken und zunehmend beeinflussen lassen, oder wir werden gegensteuern. Ich habe mich für die zweite Alternative entschieden und im Berichtszeitraum u. a. die in den beiden folgenden Artikeln beschriebenen Prüfungsschwerpunkte gesetzt.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Themen > Videoüberwachung

Videoüberwachung in Einkaufszentren: 185 Kameras überprüft

Im Rahmen einer länderübergreifenden Kontrolle von Videoüberwachungsanlagen in Einkaufszentren eines bundesweit tätigen Unternehmens habe ich drei in Niedersachsen betriebene Center mit insgesamt rund 130 Kameras überprüft.

In allen drei Centern wird die Videoüberwachungstechnik nach weitgehend einheitlicher Struktur verwendet:

- in Parkhäusern und bei Ein- und Ausfahrtschranken,
- bei Parkhaus-Kassenautomaten und Schließfächern,
- bei Notrufsäulen,
- in Anlieferzonen,
- bei Fluchtwegen und
- in den Ladenpassagen (Malls) einschließlich Rolltreppen und Vorräumen zu Aufzügen.

Videoüberwachung zur Verfolgung präventiver Zwecke nur mit Monitor und Interventionsmöglichkeit. Eine reine Aufzeichnung ist unzulässig.

Die Prüfung ergab, dass unter Berücksichtigung der vom Betreiberunternehmen vorrangig und einheitlich verfolgten Zwecke des Schutzes vor Sach- und Vandalismusschäden sowie vor Missbrauch der Notrufsäulen in diesen Bereichen (außer den Malls, siehe unten) eine Videoüberwachung nur als Monitorlösung mit Interventionsmöglichkeit, ggf. ergänzt durch eine Aufzeichnung der Videobilder, in Betracht kommen kann. Eine reine Aufzeichnung der Bilder ist hingegen unzulässig. Unter Berücksichtigung der Grundsätze der Datenvermeidung und Datensparsamkeit (§ 3 a BDSG) sollten sich die Videokameras – soweit technisch machbar – im Übrigen zum Beispiel nur dann einschalten, wenn aufgrund eines Impulses durch Betätigen des Kunden-Notrufknopfes oder durch Berühren der Parkhausschranke eine Kundenansprache oder Intervention erforderlich wird.
Hinsichtlich dieser aus der Prüfung resultierenden Empfehlungen für eine datenschutzkonforme Videoüberwachung der genannten Bereiche konnte in einer gemeinsamen Besprechung mehrerer Datenschutzaufsichtsbehörden mit Vertretern des Betreiberunternehmens weitgehend Einvernehmen erzielt werden. Deshalb gehe ich davon aus, dass die Prüfungen bereits zu einer Verbesserung der eingesetzten Videotechnik und einer nachhaltigen Einhaltung des Datenschutzes geführt haben oder noch führen werden.

Kameras müssen entfernt werden

Zum Flanieren und Verweilen einladende Bereiche müssen kamerafrei bleiben.

Keine Einigkeit konnte hingegen erzielt werden in der Frage der rechtlichen Zulässigkeit der Kameras, welche die Ladenpassagen (Malls) überwachen. Hier vertreten die Aufsichtsbehörden die Ansicht, dass diese zum Flanieren

und Verweilen einladenden Bereiche kamerafrei bleiben müssen, da in den überprüften Centern ein anzuerkennendes Erfordernis der Videoüberwachung nicht festzustellen war und ist. Da die Diskussion mit den Vertretern des Betreiberunternehmens in diesem Punkt erfolglos geblieben ist, hat die federführende Hamburger Datenschutzaufsichtsbehörde (der Sitz des Unternehmens befindet sich in Hamburg) hinsichtlich der Videoüberwachung der Malls nach § 38 Abs. 5 BDSG angeordnet, die dort verwendeten Kameras zu entfernen. Nachdem diese Entscheidung mittlerweile bestandskräftig geworden ist, hat das Unternehmen damit begonnen, alle beanstandeten Kameras abzubauen.

Weitere Kontrollen

Aufgrund der bei der Überprüfung der Einkaufscenter gemachten Erfahrungen habe ich mich entschlossen, auch die Videoüberwachungsanlagen zweier weiterer Einkaufscenter niedersächsischer Betreiber zu kontrollieren. Dabei wurden insgesamt 55 Kameras auf ihre datenschutzgerechte Nutzung und auch die technisch-organisatorische Ausgestaltung überprüft. Die Kontrollen hatten u. a. zur Folge, dass

- der Betrieb von 16 Kameras als unzulässig beanstandet wurde und diese vom Betreiber anschließend entfernt wurden,
- die Blickrichtung einer Reihe weiterer Kameras datenschutzgerecht verändert wurde,
- ein Betreiber einen bisher nicht vorhandenen betrieblichen Datenschutzbeauftragten erstmals bestellte,
- ein betrieblicher Datenschutzbeauftragter vom Unternehmen abberufen und durch einen neuen ersetzt wurde, nachdem ich wegen festgestellter unzureichender Fachkunde des Beauftragten seine förmliche Abberufung gem. § 38 Abs. 5 S. 3 BDSG angedroht hatte,
- die Betreiber nach intensiver Beratung erstmals datenschutzkonforme Verfahrensdokumentationen und Vorabkontrollen erstellten.

Die Kontrollen in allen fünf Einkaufszentren haben somit gezeigt, dass vor allem intensive Prüfungen und Beratungen „vor Ort“ zu einem datenschutzgerechten Betrieb von großen Videoüberwachungsanlagen beitragen und die Betreiber solcher Anlagen die datenschutzrechtlichen Hinweise zumeist dankbar aufgreifen. Ich werde daher die – auch anlassunabhängige – Prüfungstätigkeit in diesem Bereich künftig fortsetzen.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Themen > Videoüberwachung

Systemgastronomie: 94 Kameras in vier Restaurants

Wie in allen öffentlich zugänglichen Bereichen führt auch die Videoüberwachung in der Gastronomie immer wieder zu Beschwerden. Dabei dürfte der Branche spätestens seit einem rechtskräftigen Urteil des Amtsgerichts Hamburg vom 22.04.2008 bekannt sein, dass jedenfalls die mit Tischen und Sitzgelegenheiten ausgestatteten Gastronomiebereiche (im Fall des AG Hamburg einer Kaffeehauskette) Kundenbereiche sind, die nicht mit Videokameras überwacht werden dürfen.

Leider hat sich dies in der Systemgastronomie noch nicht allgemein herumgesprochen. So wurde ich durch eine Eingabe auf einen Franchise-Nehmer einer international tätigen Fastfood-Kette aufmerksam, der in den von ihm betriebenen vier Schnellrestaurants insgesamt nicht weniger als 94 Kameras installiert hatte. Schon wegen dieser extrem hohen Kameradichte sah ich mich bereits zu Beginn meiner Kontrolle veranlasst, auch die deutsche Konzernzentrale dieser Fastfood-Kette in die Prüfung einzubeziehen, da nicht zu erkennen war, ob der Franchise-Nehmer bei Art und Umfang des Kameraeinsatzes eigenständig oder aufgrund entsprechender Vorgaben des Konzerns gehandelt hatte. Auch das Unternehmen selbst war an einer Beteiligung interessiert. Da die Kunden regelmäßig nicht erkennen können, ob es sich um ein konzerneigenes Restaurant oder um einen Franchise-Betrieb handelt, lag es im Interesse des Unternehmens, Erkenntnisse über die Bedingungen einer datenschutzgerechten Videoüberwachung in den unter seiner Marke geführten Restaurants zu gewinnen. Aufgrund dieser Erkenntnisse wollte der Konzern dann Vorgaben für die eigenen sowie die von Franchise-Nehmern betriebenen Restaurants machen.

Die Prüfung der Restaurants des niedersächsischen Franchise-Nehmers ergab unter anderem, dass eine Vielzahl von Kameras die Sitzbereiche überwachten. Solche Bereiche, die typischerweise zum längeren Verweilen, Entspannen und Kommunizieren einladen, müssen jedoch grundsätzlich von Videoüberwachung wegen der damit einhergehenden besonders intensiven Beeinträchtigung der Persönlichkeitsrechte des Gastes frei bleiben. Daher hat das Interesse des Betreibers, die Videoüberwachung insbesondere zur Prävention vor oder zur Beweissicherung nach etwaigen Vandalismusschäden am Mobiliar verwenden zu wollen, zurückzutreten. Die mit den Konzernvertretern und dem Franchise-Nehmer in diesem Zusammenhang diskutierte Frage, ob Sitzbereiche in einem Fastfood-Restaurant zum längeren Verweilen einladen, oder ob diese Art von Lokalität nicht eher darauf ausgelegt ist, nach einer kurzen Verzehrzeit wieder verlassen zu werden, wurde schließlich einvernehmlich beantwortet: Auch der Publikumsbereich in Fastfood-Restaurants muss wegen der mittlerweile geänderten Angebotspalette, der räumlichen Umgestaltung sowie des Angebots sogenannter Lobbybereiche, die zum längeren Verweilen einladen, grundsätzlich kamerafrei sein.

Auch der Publikumsbereich in Fastfood-Restaurants muss grundsätzlich kamerafrei sein.

Aufgrund der Nähe der geprüften Restaurants zur Autobahn und zu Freizeiteinrichtungen, die in großem Maße von hauptsächlich jüngerem Publikum besucht werden, konnte jedoch das berechtigte Interesse des Betreibers am Einsatz der Kameras zur Beweissicherung insbesondere bei Sachbeschädigungen am Mobiliar nicht gänzlich unbe-

rücksichtigt bleiben. Ergebnis der Prüfung war daher, dass solche Kameras, die Sitzbereiche erfassen, die das Tresenpersonal ohne Weiteres einsehen kann, umgehend entfernt werden müssen. Dagegen dürfen zunächst die Sitzbereiche, die nicht vom Verkaufstresen einsehbar sind, für eine begrenzte Zeit weiter mit Kameras überwacht werden, um festzustellen, ob diese Bereiche tatsächlich häufig Ziel von Vandalismus sind. Sofern sich nach einer Evaluation herausstellt, dass hier nur im geringen Umfang Vorfälle zu verzeichnen waren, sind auch diese Kameras zu entfernen. Der Betreiber hat mittlerweile bereits rund 20 Prozent der auf Sitzbereiche gerichteten Kameras entfernt. Das Ergebnis der Evaluation bleibt im Übrigen abzuwarten, so dass die Prüfung fortzusetzen sein wird.

Neue Konzernregeln für Kameraeinsatz

Daneben hat die Prüfung des Franchise-Nehmers die Leitung der deutschen Konzerniederlassung dazu veranlasst, ihre bisherige Handreichung für den Einsatz von Videoüberwachungsanlagen in den unter einheitlicher Marke betriebenen deutschen Restaurants vollständig zu überarbeiten. Es wurde mittlerweile eine Richtlinie entwickelt, die sowohl für alle eigenen Restaurants wie auch für die Franchise-Nehmer verbindlich sein wird und unter anderem für neue Restaurants vorsieht, dass eine Videoüberwachung von Lobbybereichen unterbleiben muss. Für bereits bestehende Betriebe wird empfohlen, entsprechend zu verfahren. Ferner wird darin aufgrund meiner Vorgaben die Speicherdauer der Videoaufnahmen auf maximal 72 Stunden festgelegt. Damit Franchise-Nehmer bei der Einrichtung von Videoanlagen auch tatsächlich nur mit Errichterfirmen zusammenarbeiten, die die datenschutzrechtlichen Regelungen berücksichtigen, sieht die Richtlinie auch vor, diese Firmen zur Beurteilung ihrer Fachkunde vor Vertragsabschluss dem Konzern mitzuteilen.

Für die Einhaltung der datenschutzrechtlichen Regeln ist bei den konzerneigenen Restaurants der interne betriebliche Datenschutzbeauftragte zuständig. In der Richtlinie empfiehlt der Konzern auch seinen Franchisenehmern den Einsatz von eigenen betrieblichen Datenschutzbeauftragten. Hierzu werden mittlerweile konzerneigene Lehrgänge angeboten, durch die diese Personen zur Wahrnehmung ihrer Aufgaben als betriebliche Datenschutzbeauftragte befähigt werden sollen. Auch dies ist das Ergebnis der Kooperation mit mir.

Die datenschutzrechtliche Prüfung des niedersächsischen Franchise-Nehmers wird sich daher über den konkreten Fall hinaus nachhaltig positiv auf alle Videoüberwachungsanlagen dieses Unternehmens der Systemgastronomie auswirken. Da das Unternehmen zu den Marktführern seiner Branche gehört, ist zu erwarten, dass die Ergebnisse wegweisend für die gesamte Branche sein werden.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Themen > Videoüberwachung

Videoüberwachung durch Nachbarn – ein konfliktreiches Dauerthema

Neben den vorgestellten Schwerpunktthemen stellte auch die Videoüberwachung durch Nachbarn einen Tätigkeitsschwerpunkt dar. Dabei ging es zumeist um Beschwerden von Bürgerinnen und Bürgern, die sich durch Videokameras beobachtet fühlten, die Nachbarinnen oder Nachbarn zur Überwachung des eigenen Grundstücks installiert hatten.

Eine Überprüfung der vorgetragenen Sachverhalte ergab häufig, dass der Nachbar entweder nur eine Kameraattrappe verwendete oder die Videoüberwachung außerhalb von öffentlich zugänglichen Räumen erfolgte, so dass ein datenschutzaufsichtliches Einschreiten nicht in Betracht kam. In diesen Fällen, denen in der Regel ein Nachbarschaftsstreit zugrunde liegt, wird grundsätzlich auf den Zivilrechtsweg mit der Möglichkeit der Geltendmachung von Unterlassungs- und Abwehransprüchen aus den §§ 823 und 1004 BGB hingewiesen.
Bisweilen werden mit den Videoüberwachungsanlagen in der Nachbarschaft aber auch Straßen, Gehwege oder der Allgemeinheit gewidmete Gemeinschaftsflächen erfasst. Gemäß § 6 b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit Videokameras nur zulässig, soweit sie etwa zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der von der Videoüberwachung Betroffenen (z. B. Nachbarn, Passanten) überwiegen. Bereits bei der Prüfung der Erforderlichkeit der so ausgestalteten Videoüberwachungsanlagen kam ich in den meisten Fällen zu dem Ergebnis, dass die Kameras nicht datenschutzkonform betrieben wurden. Zur Erreichung des angestrebten Zwecks waren sie schlicht nicht nötig, vielmehr hätte die Installation zusätzlicher Beleuchtung mit Bewegungssensor, Alarmanlage etc. den gleichen Erfolg gehabt. In diesen Fällen wurde daher die Videoüberwachung beanstandet und eine datenschutzkonforme Neuausrichtung der Kameras oder deren Abbau verlangt.

Weitere Informationen:

www.lfd.niedersachsen.de
Pfad: Themen > Videoüberwachung

Videoüberwachung von Streikenden untersagt

Ein Fall, der auch öffentliche Aufmerksamkeit in Zeitung und Fernsehen erregte, war die Videoüberwachung von Streikenden durch den Arbeitgeber. Im Rahmen eines Streiks blockierten Streikende die sich an einer Privatstraße befindliche Zufahrt zum Werksgelände. Daraufhin ließ der Arbeitgeber im Werk zwei Videokameras aufbauen und die Menge der Streikenden kontinuierlich filmen. Er erstattete auch Strafanzeige gegen einzelne Streikende. Der Arbeitgeber, der sich rühmte, auch „unkonventionelle und unpopuläre Taktiken" anzuwenden, gab an, dass die Videoüberwachung zur Erkennung von Ausschreitungen während des Streikes gedacht sei.

Eine Prüfung dieser Videoüberwachung ergab, dass weder die formellen Voraussetzungen (gem. § 4 e BDSG Erstellen eines Verfahrensverzeichnisses, in dem u. a. der Zweck der Verarbeitung, Empfänger der Daten und Löschfristen festgelegt werden, Vorabkontrolle nach § 4 d Abs. 5 BDSG), noch die materiellrechtlichen Voraussetzungen erfüllt waren. Um Rechtsverstöße durch Ausschreitungen zu dokumentieren, wäre es ausreichend gewesen, mit der Aufzeichnung erst zu beginnen, wenn die Situation eskaliert. Ordnungsgemäß streikende Mitarbeiter unter Generalverdacht zu stellen und zu filmen, war gänzlich unverhältnismäßig.
Hinzu kam, dass sich die Streikenden durch ihre Bekleidung als Mitglieder einer Gewerkschaft kenntlich gemacht hatten. Dies hatte zur Folge, dass die Videoüberwachung zwangsläufig auch Daten über die Gewerkschaftszugehörigkeit der Streikenden erfasste. Das Merkmal der Zugehörigkeit zu einer Gewerkschaft gehört jedoch zu den „besonderen Arten personenbezogener Daten" i. S. d. § 3 Abs. 9 BDSG, die der Gesetzgeber vor dem Hintergrund der deutschen Geschichte unter besonderen Schutz gestellt hat. Gerade dieser besondere Schutz verlangt im Rahmen der Rechtsgüterabwägung nach § 32 Abs. 1 Satz 2 BDSG zwischen dem berechtigten Interesse der verantwortlichen Stelle (Arbeitgeber) und dem schutzwürdigen Interesse des Betroffenen (Streikenden) sowie den Anforderungen an die Verhältnismäßigkeit, dass hier ein hoher Maßstab an die Erforderlichkeit anzulegen ist. So war insbesondere eine lückenlose Protokollierung des Streiks völlig unverhältnismäßig.
Aus diesem Grunde habe ich die Videoüberwachung unverzüglich untersagt, die Untersagung mit einer Anordnung der sofortigen Vollziehbarkeit versehen und für den Fall der Fortsetzung der Überwachung ein empfindliches Zwangsgeld angedroht. Nahezu zeitgleich erwirkte die Gewerkschaft der Streikenden vor dem zuständigen Arbeitsgericht gegen die Videoüberwachung auf der Grundlage des Art. 9 Abs. 3 Grundgesetz (Koalitionsfreiheit) eine einstweilige Anordnung. Die Firma stellte daraufhin die Überwachung ein.

Insbesondere eine lückenlose Protokollierung des Streiks war völlig unverhältnismäßig.

Sehr enge rechtliche Grenzen

Eine Videoüberwachung von Streikenden ist nur in sehr engen rechtlichen Grenzen möglich und hat eine Reihe formeller, wie materiellrechtlicher Anforderungen zu erfüllen. Zum einen müssen sowohl ein Verfahrensverzeichnis als auch eine Vorabkontrolle vorliegen, zum anderen muss sorgfältig zwischen den berechtigten Interessen des Arbeitgebers und den schutzwürdigen Interessen der Streikende abgewogen und die Verhältnismäßigkeit und Erforderlichkeit geprüft werden. Eine Videoüberwachung Streikender kommt daher letztlich nur in Betracht, sobald Straftaten durch die Streikenden begonnen wurden oder erkennbar unmittelbar bevorstehen; selbst dann ist sicherzustellen, dass ordnungsgemäß Streikende soweit wie möglich nicht miterfasst werden.

5

Datenschutzinstitut Niedersachsen

Öffentlichkeitsarbeit, Beratung und Schulungen: Angebot und Nachfrage gestiegen

Der Schwerpunkt meiner gesetzlich festgelegten Beratungstätigkeit (§ 22 Abs. 1 NDSG) lag im Berichtszeitraum in der präventiven Beratung der öffentlichen Stellen sowohl zu materiellrechtlichen als auch technisch-organisatorischen Themen. Mittels unterschiedlicher Ansätze konnten Informationen zielorientiert vermittelt werden

- auf Veranstaltungen in den Fachbehörden vor Ort,
- in Schulungen im Datenschutzinstitut Niedersachsen (DsIN),
- in dem jährlich stattfindenden Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten,
- im Netzwerk NORD-WEST.

Die in datenschutzrechtlichen Fragen sensibilisierten Teilnehmerinnen und Teilnehmer dieser Veranstaltungen tragen als Multiplikatoren zur Entwicklung datenschutzfreundlicher Verfahrensweisen in ihren Verwaltungen bei. Die rege Nachfrage nach Schulungsveranstaltungen ist nicht zuletzt Folge der durch die Medienberichterstattung gesteigerten Aufmerksamkeit für datenschutzrechtliche Belange. Im Bereich der Presse- und Öffentlichkeitsarbeit hat der erstmalige Einsatz eines eigenen Pressesprechers seit Mitte 2009 zur Intensivierung der Medienkontakte beigetragen. Die zeitnahe Information der Medien zu aktuellen datenschutzrelevanten Themen stellt eine Serviceverbesserung für Journalistinnen und Journalisten und damit für alle Bürgerinnen und Bürger dar. Zahlreiche Anfragen von Print- und elektronischen Medien aus Niedersachsen, aus anderen Bundesländern und sogar aus dem Ausland belegen, dass das Interesse an Datenschutzthemen national wie international erheblich gestiegen ist.
Daneben wurde mit der Überarbeitung meines Internetauftritts sowie mit den dort aktuell eingestellten „Fällen aus der Praxis“ auf meiner Homepage der Informationsservice erhöht. Die auf der Website angebotenen Hinweise und Orientierungshilfen sollen dazu beitragen, die in vielen Verwaltungsbereichen gleich oder ähnlich gelagerten datenschutzrechtlichen Fragestellungen schnell beantworten zu können.

DsIN-Kurse gut angenommen

Das Schulungsangebot des bei mir angegliederten Datenschutzinstituts Niedersachsen richtet sich überwiegend an Beschäftigte der öffentlichen Verwaltung in Niedersachsen. Die aktuellen Konzepte beruhen auf der Erkenntnis, dass die meisten Datenschutzverstöße in der

Praxis nicht durch gezielte Verletzungen der Vorschriften verursacht werden, sondern überwiegend auf Unkenntnis der bestehenden Regelungen basieren, sofern es sich nicht um gezielte (strafrechtlich relevante) Angriffe unter Nutzung von Sicherheitslücken von Hard- und Software handelt. Neben der zeitnahen Vermittlung von Wissen, beispielhaften Lösungen und Werkzeugen zum Thema Datenschutz und Datensicherheit liegt der Schwerpunkt der Ausbildung in der Sensibilisierung der Teilnehmerinnen und Teilnehmer zu datenschutzgerechten Vorgehensweisen. Diese sollen in die Lage versetzt werden, als Multiplikatoren in ihren Fachbereichen das Datenschutzbewusstsein zu fördern.

Aus dem technisch-organisatorischen Bereich sind in den zwei Jahren des Berichtszeitraums verschiedenste Angebote gemacht worden. So handelt es sich zum Beispiel bei der Bausteinreihe Basiswissen für behördliche Datenschutzbeauftragte um eine vierteilige Veranstaltungsreihe. In den einzelnen Bausteinen wird sowohl das rechtliche, als auch das technisch-organisatorische Rüstzeug vermittelt, das behördliche Datenschutzbeauftragte für eine erfolgreiche Aufgabenwahrnehmung benötigen. Der technisch-organisatorische Teil nimmt dabei etwa die Hälfte der Zeit ein. Aufgrund der großen Nachfrage wurde diese Veranstaltungsreihe in jedem Jahr an drei Terminen angeboten; dennoch hat sich inzwischen eine Warteliste aufgebaut, die durch ein zusätzliches Angebot in 2011 abgebaut werden soll.

Daneben werden verschiedene Teile der Bausteinreihe wie „Ziele und Methoden des technisch-organisatorischen Datenschutzes“ sowie „Gefährdungen und Maßnahmen des technisch-organisatorischen Datenschutzes“ auch als Tagesseminare angeboten. Um auch hier der Nachfrage gerecht zu werden, wurden je Veranstaltung zwei Termine pro Jahr ausgeschrieben, die überwiegend ausgebucht waren. Darüber hinaus werden von anderen Teams verantwortete Seminare, wie „Datenschutz in Schulen“ durch Mitarbeit im technisch-organisatorischen Teil ergänzt und abgerundet.

Die Realisierung dieser erfolgreichen Fortbildungsaktivitäten binden allerdings auf Seiten des für technisch-organisatorischen Datenschutz zuständigen Teambereiches erhebliche Personalkapazitäten. Im Berichtszeitraum waren allein 36 Veranstaltungstage zu bewältigen; Zeiten für Vor- und Nachbereitung sind dabei nicht einmal berücksichtigt worden. Aufgrund der positiven Rückmeldungen soll aber trotz der engen Personalausstattung auch künftig versucht werden, die Fortbildungsaktivitäten in bisherigem Umfang weiterzuführen.

Die positive Resonanz zeigt, dass wir uns mit dem DsIN-Angebot auf dem richtigen Weg befinden und den eingeschlagenen Weg weiterverfolgen sollten.

Kursangebot des Datenschutzinstituts Niedersachsen:
www.lfd.niedersachsen.de
Pfad: Fortbildung/Informationsmaterial > Datenschutzinstitut

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

Eine sehr lohnende, wenn auch recht aufwändige Fortbildungsmaßnahme wird von meinem Technikbereich seit inzwischen fünf Jahren angeboten. Im Berichtszeitraum wurde die inzwischen etablierte Fortbildungsreihe, die als „Gesprächskreis IuK-Zukunftsentwicklung" begonnen hatte, fortgesetzt. Der Titel der Veranstaltung wurde jedoch ab 2009 angepasst. Um der Zielgruppe zu entsprechen und den Zweck als Plattform für Fragen des technisch-organisatorischen Datenschutzes von und an Experten im Leitungsbereich von Rechenzentren und IT-Servicecenters in Hochschulen, Kommunen, Landesbehörden und anderen öffentlichen Stellen gerecht zu werden, wurde als Veranstaltungstitel „Expertenkreis IT-Führungskräfte im RZ-/IT-Dienstleistungsbereich der Hochschulen und Fachhochschulen sowie von Land und Kommunen" festgelegt.

Der „Expertenkreis IT-Führungskräfte im RZ-/IT-Dienstleistungsbereich der Hochschulen und Fachhochschulen sowie von Land und Kommunen" ist im Fortbildungs-Programmheft meines Datenschutzinstituts Niedersachsen (DsIN) sowie auf meiner Website enthalten unter: www.lfd.niedersachsen.de Pfad: Fortbildung/Informationsmaterial > Datenschutzinstitut Niedersachsen (DsIN) > Programm 2011

In der Ausschreibung wurde inzwischen die Zielgruppe um die behördlichen Datenschutzbeauftragten ergänzt. Sie sind in allen Datenschutzfragen ohnehin die ersten Ansprechpartner vor Ort, wenn sich IT-Prozesse oder -Technologien ändern. Es besteht nach wie vor die Option, je nach Themenschwerpunkt die Zielgruppen zwischen Hochschulen und den übrigen öffentlichen Stellen bei Bedarf aufzutrennen oder aber gemeinsam zu tagen, wenn dies von allgemeinem Interesse ist. Erstmals 2006 und mit zwei Neuauflagen im Juni 2008 und im März 2010 wurde das relevante Themenspektrum in einer Agenda für die nächsten Sitzungen gemeinsam mit den Teilnehmenden entwickelt und fortgeschrieben. Damit wird weiterhin sichergestellt, dass eine bedarfsgerechte und vor allem zeitnahe Befassung mit technischen Innovationen am Markt und neuen Herausforderungen an IT-Sicherheit und Datenschutz erzielt wird.

Allgemein gilt (wie in allen Angeboten des DsIN), dass es nicht nur um Frontalschulung geht. Im Rahmen des Expertenkreises werden vielmehr Erfahrungen des IT-Managements beigetragen und ausgetauscht und Rahmenbedingungen und auch spezifische Lösungsansätze aus Sicht des Datenschutzrechtes sowie Erkenntnisse aus der Aufsichtstätigkeit von meiner Seite detailliert aufgezeigt. Dabei mischen sich Aspekte von juristischen, also materiellrechtlichen Datenschutz-Anforderungen mit den Erfordernissen des technischen und organisatorischen Datenschutzes.

Ziel ist es auch, neben den Beiträgen gemeinsame Überlegungen für strategische Prävention sowie wirksame datenschutzgerechte Ansätze anzustellen. Im Kern hat sich die Erkenntnis durchgesetzt: Je mehr Fragen und Anforderungen zu den komplexen Fragen des IT-Alltags im Vorfeld beratend geklärt werden können, desto weniger Fehler werden im Alltagsbetrieb auftauchen, die sich dann nur durch Beanstandungen im Prüfungsfall oder bei internen Revisionen oder Audits aufdecken und beheben lassen; eine Strategie also als eine gute Investition zur Fehlerverhütung.

Auf der Grundlage der Zielsetzung, diesen Gesprächskreis weiterhin als festen Bestandteil eines Netzwerkes zu etablieren, wurde in Abstimmung mit dem Teilnehmerkreis ein angemessener zeitlicher Rhythmus für regelmäßige Treffen gefunden. Erfreulich ist aus meiner Sicht, dass sich die inhaltliche Gestaltung dieses Weges unter stets reger Beteiligung aller Teilnehmenden fortgesetzt und weiterentwickelt hat. Ich hoffe, dass damit weiterhin ein höchstmöglicher Nutzwert aus diesem Netzwerk für die Teilnehmenden gezogen werden kann.

Auf die zehnte bis zwölfte Auflage der Veranstaltung lohnt sich eine kurze Rückschau:

10. Expertenkreis: Protokollierung II (Datenschutz & IT-Sicherheit)

- Logdaten in Applikationen und Systemen
- Protokollierung beim Accessmanagement

Rechenzentren, für IT-Anwendungen Verantwortliche und IT-Service-Einrichtungen haben ein grundsätzliches Problem. Während die Informationssicherheit eine möglichst umfangreiche Protokollierung von Systemereignissen, Zugriffsversuchen und Transaktionen fordert, um die Schutz- und Gestaltungsziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität für IT-Verfahren umzusetzen, stößt die Verarbeitung personenbezogener und personenbeziehbarer Daten auf Beschränkungen, die den Schutz von Persönlichkeitsrechten, wie das Recht auf informationelle Selbstbestimmung, gewährleisten sollen.
Daraus resultiert einerseits ein Verbot mit Erlaubnisvorbehalt nach dem NDSG, andererseits aber die Notwendigkeit, gerade im Sinne des Datenschutzes eine Protokollierung realisieren zu müssen, um die Revisionssicherheit zu gewährleisten. Der Sinn des Gebotes der Datensparsamkeit – auch und gerade von Protokolldaten – wird deutlich, wenn man sich die Szenarien des möglichen Missbrauchs (womöglich mit überbordenden Datenmengen) vor Augen führt. Die Aussagekraft von Massendaten über Verhaltensprofile, Interessenhäufung, Bewegungsprofile oder auch die „Gesinnung" lässt sich technisch durch Logdatei-Analysetools und Data Mining im Verbund mit heutiger Rechenleistung leicht nutzbar machen. Das Schadenspotential, welches ein denkbarer Missbrauch der detaillierten Rohdaten birgt, wird im Alltagsbetrieb häufig unterschätzt. Umso bedeutender ist die Frage der Dimensionierung und organisatorischen Handhabung sowie der technischen Schutzmaßnahmen von Protokolldaten, um datenschutzrechtskonform der informationellen Selbstbestimmung gerecht werden zu können.
Was also zunächst als deckungsgleiches Maßnahmenpaket von IT-Sicherheit und technisch-organisatorischem Datenschutz scheint, muss in der Praxis in jedem Fall sorgfältig und differenziert geprüft und vor dem Betrieb entsprechend den rechtlichen Anforderungen implementiert und justiert sowie organisiert werden.
Der Expertenkreis diskutierte über diese Zielkonflikte und hatte zum Ziel, Aufschluss darüber zu geben, wie rechtliche Anforderungen und Praktikabilität zusammenpassen:

- Wann ist eine Protokollierung geboten?
- In welchem Umfang, mit welcher Periodizität und mit welcher Dauer – in Abhängigkeit vom Schutzbedarf – ist sie erlaubt?

- Wann haben Löschungen oder Sperrungen zu erfolgen?
- Ab wann ist die Verarbeitung von Protokolldaten sogar verboten?
- Wie steht es mit Rechte- und Rollen-Differenzierung in der Administration und Revision?
- Welche Trennungsgebote sind zu beachten?
- Welche Konsequenzen haben die Anforderungen auf die IT-Architektur?

Aber es sind auch nicht alle technischen Szenarien gleich zu bewerten. Die Runde befasste sich auch mit den Aspekten, welche rechtlichen und technischen Unterschiede zu treffen sind bei

- Betriebssystemen,
- Authentifikations- und Autorisierungsfunktionen und im Identity-Management,
- Verzeichnisdiensten,
- Datenbanken,
- Transaktionsanwendungen,
- Web-Applikationen/Webshops/Webservern
- E-Mail-Servern,
- Proxyservern,
- Telekommunikation,
- Pay-as-you-Drive, Flugschreibern oder ähnlichen Verkehrs-Logdaten.

11. Expertenkreis: Protokollierung III (Datenschutz & IT-Sicherheit)

- Datenarten nach TKG, TMG
- „Vorratsdaten" (Speicherungspflichten von Verkehrsdaten)

Wie in allen Einzelveranstaltungen wurde der datenschutzrechtliche und technische Einstieg in den Themenbereich mit einem Initialreferat aus meinem Fachbereich für technisch-organisatorischen Datenschutz und für Datenschutz im Telemedienrecht des öffentlichen Bereiches angeboten. Neben der Definition der Datenarten nach den gesetzlichen Vorschriften des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG), galt es, die umgangssprachlichen Begriffe einzuordnen. Der so genannten „Vorratsdatenspeicherung", also den Speicherungspflichten von Verkehrsdaten nach § 113 a TKG, wurde dabei besonderes Augenmerk zuteil. Diese 11. Veranstaltungsrunde fand am 1.9.2009 statt, als die Verfassungsklage gegen diese gesetzliche Bestimmung beim Bundesverfassungsgericht anhängig war. Bereits zu diesem Zeitpunkt umfasste die kontroverse Diskussion hochaktuell die Abwägung zwischen Belangen der inneren Sicherheit und einer umfangreichen Datenspeicherung zu Gunsten der staatlichen Stellen einerseits und den Persönlichkeitsrechten einschließlich der informationellen Selbstbestimmung aller einzelnen Bürgerinnen und Bürgern anderseits. Deshalb musste die Problematik mit der teilnehmenden Zielgruppe diskutiert werden. Es konnten von meiner Seite dazu aktuelle Bewertungsergebnisse beigesteuert werden, da sich die Datenschutzbeauftragten von Bund und Ländern mit diesem Problembereich und der durch § 113 b TKG geregelten Verwendung dieser Daten durch staatliche Stellen bereits seit der politischen Planung der EU-Richtlinie und der bundesgesetzlichen Umsetzung intensiv befasst hatten. Ausweislich umfangreicher Stellung-

nahmen gegenüber dem Bundesverfassungsgericht waren sie zu einer insgesamt ablehnenden Haltung für eine anlasslose sechsmonatige Speicherung aller TK-Verkehrsdaten gelangt.
Als weiteres Feld, das sehr verbreitet Fragen zur datenschutzgerechten Handhabung aufwirft, wurde die **private Nutzung betrieblicher oder dienstlicher Kommunikationsinfrastruktur** behandelt, also der Internetzugang, die E-Mail und die Telefonie. Dabei ist die Trennung der dienstlichen von der privaten Nutzung unumgänglich, um den unterschiedlichen Anforderungen an den Datenschutz und das Telekommunikationsgeheimnis nach Artikel 10 Grundgesetz gerecht zu werden. Die gesetzlichen Bestimmungen sind bislang nicht befriedigend klar und umfassend geregelt. Bis Ende 2010 war auch noch kein gesetzgeberischer Vorstoß erkennbar, der im Rahmen des Mitarbeiterdatenschutzes eine nennenswerte Verbesserung gebracht hätte.
Um auch einen praxisorientierten Lösungsansatz zu betrachten, war eine Firma eingeladen worden, die ihr Konzept und die dazu entwickelte Produktlösung präsentierte. Die Frage, die dabei auf der Agenda stand, wurde mit **„Internet, E-Mail und Telefonie datenschutzkonform steuern"** betitelt. Es sollte geklärt werden, ob der Zielkonflikt zwischen Betriebsinteressen und informationeller Selbstbestimmung lösbar ist und wann die Aussage des Anbieters zutrifft, Kostentransparenz und Datenschutz seien vereinbar. Es wurde diskutiert, ob Telefonverhalten analysiert werden kann, ohne dass ein unzulässiger Eingriff in das Persönlichkeitsrecht erfolgt. Der technische und organisatorische Ansatz lautete, diese Kontrolle mittels Proxyweichen zu gewährleisten, indem die E-Mail- und Internet-Nutzung durch technische Trennung zwischen unternehmensbezogener und privatbezogener Nutzung erfolgt und auch die Zugriffsbefugnisse, den detaillierten Erfordernissen entsprechend angepasst, steuerbar werden. Die ausgiebige Frage- und Diskussionsrunde zeigte erneut, dass Telekommunikationsrecht und Telemedienrecht mit dem schnellen technischen und betrieblichen Wandel oft nicht Schritt halten können. Dieses Problem verstärkt sich umso mehr, wenn datenschutzrechtliche Belange mit Verfassungsrang betroffen sind, denn die Partikularinteressen der einzelnen Betroffenen – gleichgültig, ob beispielsweise Unternehmens- oder Behördenleitung, Ermittlungsbehörden, IT-Betriebsverantwortliche, IT-Sicherheitsbeauftragte – sind sehr unterschiedlich ausgestaltet. Sie kollidieren aus unterschiedlichen Gründen oft mit dem individuellen Persönlichkeitsrecht der Betroffenen.

12. Expertenkreis: Computerstrafrecht und Datenschutz

- Integrität von IT-Systemen
- „Hackerparagraf und andere Admin-Sorgen"

Die Agenda dieses umfangreichen Thementages wurde eingeleitet mit einer Themenerweiterung, die Bezug nahm auf eine bedenkliche Entwicklung der zunehmenden Hortung von Daten durch marktbeherrschende Suchmaschinenbetreiber. Einen Fachvortrag dazu hielt Dr.-Ing. Wolfgang Sander-Beuermann von der Leibniz Universität Hannover. Sein Titel **„Datensparsamkeit und Suchmaschinen: Kein Widerspruch!"** ließ die Hoffnung zu, dass es auch Lösungen oder Alternativen zu diesem problematischen Phänomen gibt.
Seit 1995 werden am Regionalen Rechenzentrum für Niedersachsen (RRZN) der Leibniz Universität Hannover Suchmaschinen entwickelt und betrieben. Bekanntestes Ergebnis dieser Arbeiten ist die deutschsprachige Meta-Suchmaschine „MetaGer", über die in vielen Fachpublikationen und Medien berichtet wurde. MetaGer ermöglicht aufgrund ihres hohen Bekanntheitsgrades und der großen Zugriffszahlen Forschung und Lehre an einem produktiven Betrieb, oder wie Dr. Sander-Beuermann sagt, am „lebenden Objekt". Dieser ist Leiter des Suchmaschinenlabors des RRZN. Sein Bericht aus dem Projekt und Produktiveinsatz von MetaGer gab Gelegenheit zum Einblick in datenschutzfreundliche Konzepte und Echtanwendungen.

In der fachlichen Auseinandersetzung konnte ein wichtiges Resümee gezogen werden: Datenspuren der Nutzer sind nur für die Vermarktung durch die gewerbliche Wirtschaft nutzbringend. Im Interesse der Nutzer dagegen steht die Datensparsamkeit und die Kontrolle über die Datenspuren im Vordergrund; dieses Interesse hat Vorrang. Daher ist die Notwendigkeit für den Betrieb von Suchmaschinen nach Interessenabwägung im Ergebnis zu verneinen. Suchmaschinen datenschutzgerecht zu implementieren, ist keine Illusion. Der beste Präventivschritt für den Schutz der Persönlichkeitsrechte ist die Datensparsamkeit und damit der Verzicht auf Cookies und auf das Speichern von IP-Nummern bei der Suchmaschinennutzung, wie dies Suchmaschinen wie MetaGer oder ixquick umsetzen.

Das Hauptthema **„Computerstrafrecht & Datenschutz: Integrität von IT-Systemen, Hackerparagraf und andere Admin-Sorgen“** wurde mit einem Initialreferat seitens meines Teambereiches für technischen und organisatorischen Datenschutz und Datenschutz im Telemedienrecht eröffnet. Informationssicherheit und technischer und organisatorischer Datenschutz erfordern organisiertes und systematisches Vorgehen. Die Maßnahmen sollen vor allem auch vor Datenmissbrauch und Angriffen durch interne oder externe Täter schützen. Aber auch Administratoren müssen die rechtlichen Möglichkeiten und Grenzen beherrschen, um nicht selbst in strafrechtlich relevante Zonen zu geraten. Wie geht das in der Praxis zusammen?

Suchmaschinenlabor des RRZN der Leibniz-Universität Hannover: http://www.rrzn.uni-hannover.de und http://www.rrzn.uni-hannover.de/sanderbeuermann.html mit der Meta-Suchmaschine https://www.metager.de/

Vortrag von Dr.-Ing. Wolfgang Sander-Beuermann: http://metager.de/FD/

Nach anfänglichen Verunsicherungen, die die neuen Strafnormen der §§ 202 c ff StGB mit sich brachten, hat sich zwar die Befürchtung relativiert, der bloße Besitz von Testsoftware, die zum Hacken und Cracken geeignet ist, sei bereits strafbar, wenn es sich um Entwickler, Administratoren und IT-Sicherheitsbeauftragte in Ausübung ihrer Profession handelt. Gleichwohl ist ein sorgsamer Umgang mit solchen Tools auch durch diesen Personenkreis erforderlich. Der Zugriff auf Produktivsysteme und Echtdaten in Filesystemen und Datenbanken unterfällt – auch für root- und adminberechtigte Funktionen – dem Datenschutzrecht. Wer die Tools mit ihren weitreichenden Möglichkeiten missbraucht, macht sich strafbar. Konkret heißt es in § 202 c: „Wer eine Straftat nach § 202 a (Ausspähen von Daten) oder § 202 b (Abfangen von Daten) vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a Abs. 2) ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“ Die Vorbereitung dieser Straftat setzt eben voraus, dass dies mit Vorsatz geschieht. Damit kann allein der Besitz der Tools zu anderen (berechtigten) Zwecken, etwa das Testen/Penetrieren und Warten von Software, nicht als Vorsatz in diesem Sinne interpretiert werden.

Die Forschung und Förderung alternativer Suchmaschinen wird von dem gemeinnützigen **SuMa-eV** – Verein für freien Wissenszugang betrieben. http://suma-ev.de/wsb/ . Dieser hat die Entwicklung der Suchmaschinen mit MetaGer2 weitergetrieben. Das Metager2-Projekt wirbt mit dem Anspruch: „Schach den Datenkraken: KEINE Speicherung Ihrer Daten bei Metager2!“ https://metager2.de/

SuMa-eV ist seit 1.12.2007 auch beauftragt für Entwicklung und Betrieb der Suchmaschine für Verbraucher „Clewwa“ http://clewwa.de/ beim Bundesamt für Verbraucherschutz und Lebensmittelsicherheit

Um die Sichtweise im Bereich des **Computerstrafrechts aus dem Blickwinkel der polizeilichen Praxis** zu betrachten, referierte Dr. Susanne Graf von der Polizeidirektion Braunschweig, Dezernatsleiterin 22 (Justiziariat/Recht) hierzu. Als Strafrechtlerin/Expertin für IuK-Kriminalität und Dozentin an der Polizeiakademie Niedersachsen verfügte sie über die Veranstaltung bereichernde Erfahrungen: Sie beleuchtete die juristischen Grundlagen der Delikte rund um die IT aus der Sicht von Ermittlungsbehörden.

Inzwischen hat der Anteil der Delikte erheblich zugenommen, die im Internet stattfinden oder bei denen das Internet Tatmittel ist. Sehr oft sind die Computer und andere informationstechnische Systeme als Spurenträger für die Beweisführung relevant. Digi-

tale Spuren sind Protokolle in den vielfältigsten Formaten und Zusammenhängen. Um diesen Zusammenhang – auch mit Datenspuren als Aktivitäten-, Kommunikations- oder Bewegungsprotokoll – zum Datenschutz zu beleuchten, referierte Christian Lange vom Landeskriminalamt Niedersachsen, Dezernat 56 Forensische IuK/Zentrale DV-Gruppe zum Thema **„IT-Forensik: Datenspuren auf Datenträgern und in Informationssystemen".** Dabei interessierten den Teilnehmerkreis Fragen zur Verlässlichkeit und Sicherheit von physischen und logischen Löschfunktionen von Daten, zur Rekonstruierbarkeit von Datenspuren, die Aktivitäten in Informationssystemen generell hinterlassen, und zu den forensischen Möglichkeiten, die Systemverantwortliche haben, um Angriffe zu lokalisieren und beweisfähig zu dokumentieren.
Wie viele rekonstruierbare Datenspuren alle Aktivitäten in Informationssystemen generell hinterlassen, wurde an folgenden Beispielen verdeutlicht:

- Spuren auf Datenträgern (z. B. im Cache, in Cookie-Dateien, in Flash-Cookies, in der Browser History),
- programmeigene Protokolle (z. B. Chat-Protokoll),
- Projektdateien, also wieder verwendbare Zusammenstellungen für einmal erzeugte Brennprogramme, Registry-Datenbank des Windows-Betriebssystems,
- Mounted Devices (virtuelle Laufwerke), Druckerspool mit Druckaufträgen und Metadaten,
- Vermeintlich gelöschte (aber nicht vom Dateisystem tatsächlich überschriebene) Dateien,
- NTFS-Reparse Points, Volumenschattenkopien,
- Voransichten zu Grafikdateien (Thumbnaildateien „thumbs.db"),
- Transaktionslogdateien,
- Spuren in Logdateien von Servern (z. B. Web, FTP, Mail),
- Spuren in Logdateien auf Clients (z. B. Process-Accounting),
- Spuren in Logdateien von Drittsystemen (z. B. Intrusion Detection Systems zur automatisierten Erkennung von Angriffen auf Netzwerke, Provider-Datenbestände wie Transfervolumen oder IP-Adressen).

Weitere Suchmaschine mit datenschutzfreundlichem Konzept: https://www.ixquick.com/

Auditierung, Revision und die Schutzziele ähneln sich an vielen, wenn auch nicht an allen Stellen: Technisch-organisatorischer Datenschutz und Informationssicherheit haben eine gemeinsame Schnittmenge bei der Zielsetzung und im methodischen Vorgehen. Um die Synergiemöglichkeiten zwischen systematischem Datenschutz und IT-Sicherheit auszuschöpfen, referierte zum Thema **„Systematische Informationssicherheit in großen Organisationen"** Heinz Petersen von der Zentralen Polizeidirektion (ZPD), Abteilung 4 (Polizeitechnik). Er ist Beauftragter für Informationssicherheit der Polizei des Landes Niedersachsen. Informationssicherheits-Managementsysteme (ISMS) sollen die professionelle Grundlage liefern, um Prävention und Intervention gegen Hacking und andere Sicherheitsvorfälle zu ermöglichen und zu organisieren. Der Vortrag beleuchtete unter anderem, welche strategischen und taktischen Methoden und welche operativen Werkzeuge und Praxis-Tools in den Alltag gehören.

Resümee:

In Abstimmung mit dem Kreis der Teilnehmenden soll die Agenda weiterentwickelt werden. Die kontinuierliche Fortsetzung und die engagierte Teilnahme der Fachleute sowie das Podium mit Referenten unterschiedlicher Forschungseinrichtungen und IT-Firmen hat bereits zu einer Etablierung im Datenschutzinstitut für die Fragen des technischen Datenschutzes und des Telemedienrechtes geführt und wird für weitere Planungen prägend sein. Trotz des erheblichen und sehr individuellen fachlichen Vorbereitungsaufwandes wird das LfD-Technikteam diese Veranstaltungsreihe des Expertenkreises in einem sachgerechten zeitlichen Rhythmus fortsetzen. Leider ließ sich aus Gründen des Personalmangels eine Verdichtung der Tagungsfolge bisher nicht leisten.

CHARTA DER GRUNDRECHTE DER EUROPÄISCHEN UNION
proklamiert in Nizza am 07. 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.

Der Landesbeauftragte für den Datenschutz Niedersachsen