daten
schutz

XVIII. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2005 – 2006

Herausgeber: Der Landesbeauftragte für den Datenschutz Niedersachsen
~~Brühlstraße 9, 30169 Hannover~~ Prinzenstr. 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.

XVIII. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2005 – 2006

Inhaltsverzeichnis

Zu diesem Bericht

Die Broschüre, die Sie gerade in Händen halten, ist der Tätigkeitsbericht des Niedersächsischen Landesbeauftragten für den Datenschutz, der – schon zum 18. Mal – gesetzesgemäß im 2-Jahres-Rhythmus dem Niedersächsischen Landtag vorzulegen ist.

Für den Berichtszeitraum 2005–2006 ergibt sich dabei eine Besonderheit: In der Zeit vom 1.1.2006 bis zum 31.1.2007 hatte die Niedersächsische Landesregierung die Aufgaben des nicht-öffentlichen Datenschutzes – also vor allem im Bereich der Wirtschaft – dem Ministerium für Inneres und Sport übertragen.
Es besteht Einvernehmen, dass ich auch die „Ministerialzeit" übernehme und der Bericht „aus einem Guss" mit informeller einmonatiger Verlängerung verfasst werden kann.
Unabhängig davon sind die nachfolgenden Fachbeiträge bis zum Redaktionsschluss im Sommer aktuell gehalten worden, um zu vermeiden, dass die Texte schon bei Erscheinen hier und da überholt sind.
Zielsetzung des Vorhabens war es nicht nur, einen schwerpunktorientierten Überblick über die geleistete Arbeit zu geben, sondern – mehr vielleicht als bisher – zu informieren über die aktuelle Situation des Datenschutzes in der niedersächsischen Wirtschaft, Verwaltung und Bevölkerung.
Den Schwerpunkt bildet diesmal – schon an der Seitenzahl erkennbar – der Fachbeitrag zur technisch-organisatorischen Seite des Datenschutzes. Die Informationstechnologie nimmt einen immer breiteren Raum in der Berufswelt, aber auch im Privatleben ein – und das bei ständig zunehmendem Innovationstempo. Der Fachbeitrag stellt den Versuch dar, einen konzentrierten Einblick in dieses Gebiet in einer Weise zu verschaffen, die schon einem interessierten, nicht aber erst einem darauf spezialisierten Leserkreis gerecht wird.
Ich bin auf Ihre Reaktion gespannt …

Die äußere Gestaltung des Berichts folgt der erstmals für die Jahre 2003–2004 modernisierten Linie (sog. management summary), die ein durchweg positives Echo hatte.
Die früher vorzufindende Sammlung von Einzelfällen ist also nicht mehr enthalten. Ich habe mir vorgenommen, statt dessen eine Zusammenstellung allgemein interessanter Fälle aus der niedersächsischen Datenschutzpraxis in vereinfachter, natürlich anonymisierter Form aufzubauen und die Datei mit der Möglichkeit der Volltextsuche im Internet zur Verfügung zu stellen.
Damit stehen die Informationen für jeden Interessierten nicht erst nach einer Zeit von bis zu zwei Jahren, sondern relativ zeitnah bereit.

Beim Durchblättern werden Sie verschiedene Darstellungsstile finden, vom klassischen Bericht über dialogisch angelegte Teile bis zum kleinen Dossier.
Ich erhoffe mir durch den Stilmix einen leichteren Zugang bei der Lektüre der folgenden Seiten und danke für Ihr Interesse.

Joachim Wahlbrink
Landesbeauftragter für den Datenschutz

Was nicht in den Fachberichten steht …

Datenschutz ist eigentlich nicht das richtige Wort. Er ist nur ein Zwischenziel auf dem Weg zum Schutz der Privatsphäre des Einzelnen. So ist im englischen Sprachgebrauch auch zutreffender von privacy protection die Rede.
Der Schutzbedarf ist ein individuelles Kriterium: Der eine „hat nichts zu verbergen“, ein anderer sieht sich überall beobachtet, belauscht, im Ergebnis regelrecht ausspioniert.
Doch unabhängig von den persönlichen Befindlichkeiten gilt für uns alle, dass wir durch die Erfassung unserer Daten mehr oder weniger manipulierbar oder auch tatsächlich manipuliert werden.
Mit dem Menschenbild des Grundgesetzes ist das nicht vereinbar.
Der überpersonale öffentliche Durchsetzungsanspruch des Datenschutzgedankens findet sich in den Datenschutznormen in der Europäischen Union, der Bundesrepublik Deutschland und der Bundesländer verteilt.
Danach ist der Schutz der Privatsphäre bei uns ein verfassungsrechtlich garantiertes Grundrecht. Es kann in Konkurrenz zu anderen Grundrechten stehen, vor allem zu Schutzgütern wie Leben, Gesundheit und Freiheit.
Die dann nötige Güterabwägung ist in erster Linie den Parlamenten in die Hände gelegt – eine schwere und sehr verantwortungsvolle Aufgabe.
Insbesondere der Bereich der öffentlichen Sicherheit, die Vollmachten für Polizei und Verfassungsschutz haben seit einigen Jahren gegenüber den Datenschutzinteressen meist das größere politische Gewicht. Dieser Umstand ist nicht nur aus datenschutzrechtlicher Sicht fatal und zu bedauern. Er birgt mittel- und langfristig große Risiken. Eine Gewöhnung weiter Teile der Bevölkerung an immer schärfere Grundrechtseingriffe, die Verkümmerung der Bürgerrechte, stellen die größten Errungenschaften des Grundgesetzes in Frage.
Die praktischen Folgen dieser Bewegung sind unabsehbar. Vergleiche mit historischen Vorläufern hinken natürlich – ermutigend sind sie jedoch in keinem Fall.
Dennoch sehe ich mich nicht als Rufer in der Wüste .
Deutschland ist keine Datenschutzwüste. Im internationalen Vergleich stehen wir – noch – gut da.
Mit zunehmenden Eingriffen in die Privatsphäre kann auch der Widerstand wachsen. Nach meinem Eindruck reagiert die Öffentlichkeit, besonders die Presse, schon kritischer als bislang. Journalisten sind nicht zuletzt auch beruflich und privat mitbetroffen.
Damit nicht die bloße Angst die Weichen stellt, sind umfassende Aufklärung und offene öffentliche Diskussion unverzichtbar. Deshalb wird die Öffentlichkeitsarbeit, vor allem der bürgerrechtlich orientierten Verbände immer wichtiger. Gleiches gilt natürlich auch für die Datenschutzbeauftragten.
Ein kleines Stück davon soll dieser Bericht sein.

1 Datenschutz in der Wirtschaft

Datenschutzaufsicht im nicht öffentlichen Bereich

Seit Februar 2007 bin ich auch wieder für den Datenschutz im nicht öffentlichen Bereich zuständig. Ich habe daher auf der Grundlage des Bundesdatenschutzgesetzes Unternehmen zu beraten und zu kontrollieren, die in Niedersachsen ihren Sitz haben, und auf die Beachtung der datenschutzrechtlichen Vorschriften durch diese Unternehmen hinzuwirken. Dazu können auch Prüfungen vor Ort erfolgen, Stellungnahmen eingeholt oder datenschutzrechtliche Maßnahmen angeordnet werden. Besonderen Stellenwert hat jedoch die Beratung. An mich können sich Unternehmen, betriebliche Datenschutzbeauftragte und Bürger wenden, wenn Klärungen zur Rechtmäßigkeit der Datenverarbeitung erfolgen sollen. Auch Beschwerden über Datenschutzverstöße können gemeldet werden.

Kundendaten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen.
Diese beiden Begriffsbestimmungen sollen den Geltungsbereich des Gesetzes grob darstellen.

Fast täglich wenden sich Bürgerinnen und Bürger an mich, die verunsichert sind, wenn sie einer Datenverarbeitung zustimmen sollen, die sie nicht verstehen. Manche Bürger ärgern sich über die Werbung im Briefkasten, die direkt an sie adressiert ist und andere wundern sich, warum eine Auskunftei ihre Daten ohne Genehmigung weitergibt.
Zu den häufigsten Fragen und Problemen, wie z. B. unverlangte Werbung oder die Tätigkeit von Auskunfteien, biete ich bereits auf meiner Internetseite umfangreiches Informationsmaterial an, dass anlässlich des Aufgabenübergangs wieder grundlegend aktualisiert wurde. Da viele Bürgerinnen und Bürger das Internet als wichtigste und am leichtesten zugängliche Informationsquelle nutzen, wird das Angebot ständig erweitert werden.

Schutz der eigenen Daten

Da das Datenschutzrecht sich aus dem Persönlichkeitsrecht entwickelt hat, ist die Eigenverantwortlichkeit oberster Grundsatz im Datenschutzrecht. Die Betroffenen sollten deshalb sehr verantwortungsbewusst und kritisch mit den eigenen Daten umgehen. Es wird daher empfohlen:

- Nur erforderliche Daten in Formulare eintragen
- Keine Gewinnspiele oder Preisausschreiben mitmachen
- Bei Bestellungen sofort der Werbung widersprechen
- Einwilligungserklärungen genau durchlesen und Ungewolltes streichen
- Bei Kundenkarten prüfen, ob sich der Rabatt angesichts eines entstehenden Kundenprofils lohnt
- Bei Fragen zum Datenschutz sich an den betrieblichen Datenschutzbeauftragten oder an den Landesbeauftragten für den Datenschutz wenden

Rechte des Betroffenen

Aus vielen Anfragen wird deutlich, dass die Bürgerinnen und Bürger ihre Rechte als Betroffene nicht kennen. Darüber hinaus werden diese vielfach auch von den Unternehmen nicht beachtet. Zu den Rechten der Betroffenen gehört das Recht auf Auskunft, Berichtigung, Sperrung und Löschung.

Der Betroffene kann nach dem BDSG Auskunft verlangen über die zu seiner Person gespeicherten Daten, deren Herkunft, die Empfänger oder Empfängerkategorien sowie den Zweck der Speicherung. Bei Auskunfteien kann der Betroffene Auskunft über Herkunft und Empfänger nur verlangen, sofern nicht das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. Falsche Daten hat das Unternehmen zu berichtigen. Nicht mehr erforderliche Daten sind zu löschen bzw. zu sperren. Bestrittene Daten sind bis zur Klärung zu sperren.
Der Datennutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung kann der Kunde jederzeit widersprechen. Damit wird die Datennutzung für diese Zwecke unzulässig.

Kundendaten bei Firmenzusammenschlüssen

Im vergangenen Berichtszeitraum hat die niedersächsische Aufsichtsbehörde für den Datenschutz sich eingehend mit den Fragen zur Datenverarbeitung bei Unternehmenszusammenschlüssen beschäftigt. Ein großer, europaweit tätiger Finanzdienstleister wurde von einem international tätigen Konzern in der Form einer erheblichen finanziellen Beteiligung übernommen. Nunmehr sollten Synergieeffekte genutzt werden und die Kundendaten möglichst schnell und umfassend beiden Unternehmensgruppen zur Verfügung gestellt werden. Weil das niedersächsische Unternehmen bereits aus einer früheren Übernahme und dem damals erfolgten Kontakt mit der Aufsichtsbehörde für den Datenschutz Erfahrung gesammelt hatte, wurde auch jetzt die Datenschutzaufsicht frühzeitig in die Maßnahmeprüfung und Entscheidungsfindung einbezogen.
Dies gibt Anlass, über die Modalitäten bei Firmenzusammenschlüssen zu informieren:

Rechtsgrundlagen

Es gibt kein Konzernprivileg im Datenschutzrecht, andere Konzernunternehmen gelten grundsätzlich als „Dritte". Datenweitergaben an andere Konzernunternehmen sind daher datenschutzrechtlich als Übermittlungen zu qualifizieren und dürfen nur erfolgen, wenn eine Rechtsgrundlage dafür vorliegt oder der Betroffene eingewilligt hat.
Zunächst sind Datenverarbeitungen im Rahmen des § 28 Abs. 1 Nr. 1 BDSG zur Erfüllung eigener Geschäftszwecke für die Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen zulässig. Zudem ist eine Datenverarbeitung zulässig, die zur Wahrung berechtigter Interessen des Unternehmens erforderlich ist, und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt (§ 28 Abs. 1 Nr. 2 BDSG).
Diese Regelungen erlauben den Unternehmen die Datenverarbeitung zur Fortführung der Vertragsverhältnisse und entsprechen damit den Interessen beider Vertragspartner. Die Kundenstammdaten können darüber hinaus in gemeinsamen Datensammlungen gespeichert und den jeweiligen Unternehmen, mit denen eine Vertragsbeziehung zum Kunden besteht, zur Verfügung gestellt werden. Damit soll die richtige Zuordnung des Schriftverkehrs bzw. bei telefonischen Anfragen die richtige Zusteuerung an die Unternehmen der Unternehmensgruppe bzw. des beteiligten Konzerns ermöglicht werden. Die angeschlossenen Unternehmen erhalten die Daten also ausschließlich zum Zwecke

der ordnungsgemäßen Vertragserfüllung. Die zentrale Speicherung und Datenpflege stellt die Aktualität dieser Daten sicher und erreicht damit Effizienzsteigerungen sowie Kostenersparnisse.
Weiterhin ist eine Datenübermittlung oder -nutzung für einen anderen Zweck gem. § 28 Abs. 3 Satz1 Nr. 1 BDSG zulässig, soweit es zur Wahrung berechtigter Interessen eines Dritten erforderlich ist und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.
In den letzten Jahren kam es zu einer größeren Zahl von Fusionen und Zusammenschlüssen zwischen Banken, Finanzdienstleistern und/oder Versicherungen. Im Rahmen einer Fusion ist das Umwandlungsgesetz (UmwG) anzuwenden. Nach § 20 UmwG kommt es bei einer Verschmelzung i. S. v. § 2 UmwG bzw. mit der Registereintragung zu einer Gesamtrechtsnachfolge. Das neu entstandene oder das eine andere Firma übernehmende Unternehmen tritt als Gesamtrechtsnachfolgerin für das Vorgängerunternehmen in die Verträge zu den Kunden ein und ist damit nicht Dritte im Sinne des Bundesdatenschutzgesetzes. Eine Datenübermittlung findet daher nicht statt.

Einwilligung

Auch im Rahmen eines Verbundes bzw. einer Partnerschaft von Unternehmen können Datenübermittlungen erforderlich sein. Diese umfasst die gesamte Datenverarbeitung auf Konzernebene und die Finanzdienstklausel, also die Klausel, wonach der Vermittler die allgemeinen Antrags-, Vertrags- und Leistungsdaten auch für die Beratung und Betreuung in sonstigen Finanzdienstleistungen nutzen darf. Dies kann nur mit Einwilligung der Kunden geschehen.

Schriftform der Einwilligungserklärung

Nach § 4a Abs. 1 Satz 3 BDSG bedarf die Einwilligung der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.
Einen solchen Ausnahmetatbestand sah die Aufsichtsbehörde in dem oben genannten Fall als gegeben an. Hier sollte der bisher vom Finanzdienstleister durch eigene Berater wahrgenommene Kundendienst in einer neu gegründeten Gesellschaft aufgehen, die die Beratung für alle Konzernunternehmen wahrnehmen soll. Die Datenverarbeitung im Gesamtkonzern auf eine einheitliche Grundlage zu stellen war als berechtigtes Interesse anzuerkennen, da sonst bei der Datenverarbeitung etliche unterschiedliche Einwilligungserklärungen berücksichtigt werden müssten. Eine ordnungsgemäße Vertragsbearbeitung und eventuelle Widerspruchsberücksichtigung würde erheblich erschwert werden.
Bei der Umsetzung von Fusionen und Zusammenschlüssen sollte eine einheitliche Einwilligungserklärung in den Vertragsbeständen gelten und die Kunden durch Informationen auf die jederzeitige Widerspruchsmöglichkeit hingewiesen werden. Wegen der Vielzahl der betroffenen Verträge war diese Lösung eine an Stelle der Schriftform angemessene Alternative. Die einheitliche Datenverarbeitung und Vertragsführung wäre gerade auch in Erwartung einer geringen Rücklaufquote der abzugebenden Einwilligungen infrage gestellt. Da Zusammenschlüsse und Fusionen von Unternehmen rechtlich gestaltet werden können, kann anderseits dies nicht von der datenschutzrechtlichen Einwilligung eines jeden Kunden abhängig sein.

Im Ergebnis beeinträchtigt die Widerspruchslösung die Betroffenen auch nicht in unangemessener Weise, wenn die Klausel wie in dem hier entschiedenen Fall keine grundlegenden Änderungen erfahren hat und eine umfassende Information erfolgt. Zu betonen ist jedoch, dass es sich um eine Einzelfallentscheidung handelt. Eine enge Abstimmung mit der Aufsichtsbehörde ist daher den Unternehmen in jedem Fall zu empfehlen.

Informationen und Widerspruchslösung

Um die Verarbeitung der Daten und der möglicherweise eingelegten Widersprüche zur Datenverarbeitung auch sicher und konsequent durchführen zu können, müssen die Unternehmen ihre Kunden über den Zusammenschluss sowie über die Vereinheitlichung der Einwilligungserklärung informieren und auf das Recht, dieser Verfahrensweise innerhalb einer bestimmten angemessenen Frist zu widersprechen, hinweisen. Die neue Klausel ersetzt die in den einzelnen zusammengeschlossenen Unternehmen bisher verwendete Einwilligungsklauseln, welche bereits Inhalt der vertraglichen Beziehung mit den Kunden war.
Der Betroffene kann Widerspruch gegen eine Datenübermittlung an:

- den übernehmenden Konzern
- Berater/Partner (insgesamt und einzeln)
- für Werbung

gesondert einlegen. Die Widersprüche werden von den betrieblichen Datenschutzbeauftragten der jeweiligen Unternehmen bearbeitet. Über Kennzeichnungen und Berechtigungskonzepte wird z. B. die Sperrung der Daten oder der Werbestopp sichergestellt.
Wenn der Kunde der Weitergabe seiner Daten an andere Konzernunternehmen widerspricht, dürfen sie nur für die ordnungsgemäße Erfüllung der Vertragsangelegenheiten verarbeitet werden. Der Widerspruch darf keine negativen Auswirkungen auf das Vertragsverhältnis des Kunden haben.
Die Befreiung vom so genannten Bankgeheimnis ist erforderlich, wenn der Kunde die Beratung und Betreuung durch den zuständigen Berater auch in sonstigen Finanzdienstleistungen wünscht.

Weitere Konsequenzen für die Unternehmen

Durch die Einbeziehung des gesamten Außendienstes und der Fachberater für datenschutzrechtliche Fragen der Kunden sollte eine intensive Gesprächsebene für die Betroffenen geschaffen werden. So können den Mitarbeitern des Vertriebes bereits im Vorfeld Datenschutzschulungen angeboten und schriftliches Material zur Verfügung gestellt werden. Die eingelegten Widersprüche sollten zügig bearbeitet werden und den Betroffenen eine schriftliche Bestätigung zukommen.

Versicherungswirtschaft – Schweigepflicht-Entbindungserklärung bei privaten Krankenversicherungen 2

Im Berichtszeitraum erreichten die Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich zahlreiche Beschwerden über die Praxis von privaten Krankenversicherungen, im Falle eines Leistungsantrages Auskünfte bei den behandelnden Ärzten einzuholen. Ärzte und Zahnärzte sind verunsichert: Sie erhalten Anfragen von privaten Krankenversicherungen zu einem Patienten mit der Mitteilung, der Patient habe sie von der Schweigepflicht entbunden. Die Schweigepflichtentbindungserklärung wird meist nicht vorgelegt, ihr Umfang ist für den Arzt nicht erkennbar. Teilweise würden umfangreiche Auskünfte gefordert, ohne dass der konkrete Anlass der Erhebung offen gelegt werde.
Die Versicherungen haben ein legitimes Interesse, im Versicherungsfall die Berechtigung einer Forderung überprüfen zu können. Dass sie für diese Zwecke Gesundheitsdaten ihrer Versicherten benötigen, unter anderem Patientendaten, die bei den Ärzten bzw. Zahnärzten vorhanden sind, steht außer Frage. Diese Daten unterliegen jedoch dem strafrechtlich in § 203 Abs. 1 Nr. 1 Strafgesetzbuch und standesrechtlich in den Berufsordnungen der Ärztekammern geschützten Patientengeheimnis. Daher benötigt der Arzt Rechtssicherheit, um zu vermeiden, dass er standesrechtlich oder gar strafrechtlich zur Rechenschaft gezogen wird.
Datenschutzrechtlich ist die Übermittlung von Patientendaten an die Versicherung nur zulässig, wenn eine gesetzliche Regelung dies gestattet oder der Betroffene eingewilligt hat. Eine gesetzliche Übermittlungsbefugnis gibt es anders als beim Datenfluss zwischen Ärzten und gesetzlichen Krankenkassen nicht. Die Versicherungen berufen sich auf eine im Jahre 1989 mit den Datenschutzaufsichtsbehörden abgestimmte und bei Vertragsschluss zu unterzeichnende Klausel mit folgendem Wortlaut, der zum Teil leicht verändert wird:

Mir ist ferner bekannt, dass der Versicherer zur Beurteilung seiner Leistungspflicht auch Angaben überprüft, die ich zur Begründung etwaiger Ansprüche mache oder die sich aus von mir eingereichten Unterlagen (z. B. Rechnungen, Verordnungen) sowie von mir veranlassten Mitteilungen eines Krankenhauses oder von Angehörigen eines Heilberufs ergeben. Auch zu diesem Zweck befreie ich die Angehörigen von Heilberufen oder Krankenanstalten, die in den vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht; dabei hat die Geltendmachung eines Leistungsanspruches die Bedeutung einer Schweigepflichtentbindung im Einzelfall. Von der Schweigepflicht entbinde ich auch zur Prüfung von Leistungsansprüchen im Falle meines Todes. Die Schweigepflichtentbindung für die Leistungsprüfung bezieht sich auch auf die Angehörigen von anderen Kranken- und Unfallversicherern, die nach dort bestehenden Versicherungen befragt werden dürfen.

Zwischenzeitlich hat sich die rechtliche Beurteilung dieser Schweigepflichtentbindungserklärung durch die Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich geändert. Dem Gesamtverband der Versicherungswirtschaft (GDV) ist seitens des Düsseldorfer Kreises (Abstimmungsgremium der obersten Datenschutzaufsichtsbehörden des Bundes und der Länder), vertreten durch den Hamburgischen Datenschutzbeauftragten, bereits 2004 mitgeteilt worden, dass bei eingereichten Leistungsanträgen für Rückfragen bei Ärzten, Krankenhäusern und auch anderen Versicherungsgesellschaften jeweils eine Schweigepflichtentbindungserklärung vom Versicherungsnehmer für den Einzelfall einzuholen ist.

Rechtliche Vorgaben für die Schweigepflichtentbindungserklärung

Die gesetzlichen Anforderungen an eine wirksame Einwilligungserklärung ergeben sich aus § 4a BDSG. Danach ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht und er auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hingewiesen worden ist.
Diesen Anforderungen entspricht die von der Versicherungswirtschaft verwendete Klausel nicht. Sie enthält eine pauschale, auf die Zukunft gerichtete Entbindung von der Schweigepflicht. Bei Abgabe der Erklärung ist dem Betroffenen weder der Name des Arztes, noch der Anlass für eine künftige Behandlung bekannt, so dass sich die Einwilligungserklärung nicht auf konkrete Gesundheitsdaten beziehen kann. Ein wirksamer Kontrollmechanismus für die Erforderlichkeit der Datenerhebung durch die Versicherung fehlt damit. Außerdem kann eine Einwilligungserklärung nur ausdrücklich, nicht aber fiktiv mit der Geltendmachung eines Leistungsanspruches abgegeben werden. Die Verwendung der Klausel wurde daher in den konkreten Fällen beanstandet. Die privaten Krankenversicherungen in Niedersachsen wurden über die Rechtslage unterrichtet und gebeten, künftig Schweigepflichtentbindungserklärungen bezogen auf den konkreten Einzelfall einzuholen. Zu begrüßen ist, dass das Bundesministerium der Justiz in seinem Entwurf eines Gesetzes zur Reform des Versicherungsvertragsrechts eine Regelung zur Erhebung personenbezogener Gesundheitsdaten bei Ärzten aufgenommen hat, wonach eine Einwilligung nach § 4a BDSG im Einzelfall erteilt werden muss.

Bundesverfassungsgericht stärkt Versichertenrechte

1 BvR 2027/02

In seinem Beschluss vom 23. Oktober 2006 hat das Bundesverfassungsgericht die Versichertenrechte erheblich gestärkt. In einem die Berufsunfähigkeitsversicherung betreffenden Fall hielt es die pauschale Entbindungspflicht für unvereinbar mit dem Recht auf informationelle Selbstbestimmung des Versicherten, wenn zwischen dem Versicherer und dem Betroffenen ein erhebliches Verhand-

lungsungleichgewicht bestanden habe und die Klausel nicht verhandelbar gewesen sei, so dass dem Versicherungsnehmer als Alternative nur ein Verzicht auf den Vertragsschluss verbleibe. Das Gericht rügte insbesondere die weite Fassung der Erklärung, in der weder bestimmte Auskunftstellen noch bestimmte Auskunftsersuchen bezeichnet sind, so dass praktisch nicht absehbar sei, welche Auskünfte von wem eingeholt würden. Da auch die Ärzte faktisch oft nicht in der Lage seien, die Sachdienlichkeit der Anfrage zu prüfen, fehle ein wirksamer Kontrollmechanismus.

Künftige Entwicklung

Die Versicherungswirtschaft hat aufgrund der Reform des Versicherungsvertragsrechts bis Anfang 2008 neue Vertragsunterlagen zu erstellen. Die Datenschutzaufsichtsbehörden des Bundes und der Länder werden in der Arbeitsgruppe Versicherungswirtschaft des Düsseldorfer Kreises, in der seit Anfang 2006 auch Niedersachsen (seit 1.2.2007 der Landesbeauftragte für den Datenschutz) aktiv mitwirkt, die Entwicklung datenschutzkonformer Muster-Einwilligungserklärungen durch den GDV beratend und unterstützend begleiten.

Die Neuerungen des Bundesdatenschutzgesetzes – nur eine Entlastung für den Mittelstand?

Durch das „Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft“ vom 22. August 2006 hat das Bundesdatenschutzgesetz eine Reihe von Änderungen erfahren, die sich in der Praxis wesentlich auf den Schutz personenbezogener Daten und die Kontrolle ihrer Verarbeitung auswirken wird.

Zielsetzung der Änderungen

Der Datenschutz im nicht-öffentlichen Bereich, der seit 1. Februar 2007 wieder in meinem Zuständigkeitsbereich liegt, basiert im Wesentlichen auf den Regelungen des Bundesdatenschutzgesetzes (BDSG). Das BDSG ist im letzten Jahr in einigen wichtigen Punkten geändert worden. Intention des Bundesgesetzgebers war die „Abschaffung unnötiger Vorschriften“ zur Beseitigung der bestehenden „kostenträchtigen Überregulierung“, da diese als verantwortlich für die „derzeitige strukturelle Wachstumsschwäche“ ausgemacht wurde. Im Rahmen des Programms „Bürokratieabbau und bessere Rechtsetzung“ wollte man mit dieser Gesetzesänderung insbesondere Mittelständler und Existenzgründer entlasten.
Weiterhin war beabsichtigt, die Position der externen Datenschutzbeauftragten zu präzisieren, da das bisher geltende Recht kein Zeugnisverweigerungsrecht und Beschlagnahmeverbot für externe Datenschützer bei verantwortlichen Stellen mit besonderen Geheimhaltungspflichten (Ärzte, Anwälte) vorsah. Damit war die Berufung eines externen Datenschutzbeauftragten bei diesen Stellen nur mit Einschränkungen möglich, weil die der besonderen Schweigepflicht unterliegenden Daten nur von einem Angehörigen des entsprechenden Berufsstandes geprüft werden konnten.
In diesem Zuge wurden die korrespondierenden Regelungen des Strafgesetzbuches (§ 203: „Verletzung von Privatgeheimnissen“) angepasst, indem diese Regelungen auf den Datenschutzbeauftragten ausgedehnt wurden, wobei er gleichzeitig ein Zeugnisverweigerungsrecht für Kenntnisse die er im Rahmen der Prüfung dieser Daten erlangt hat, erhielt. In gleicher Weise wie beim Angehörigen einer der o. g. Berufsgruppen, sind die Daten auch im Besitz des Datenschutzbeauftragten vor Beschlagnahme geschützt.

3

Auswirkungen im Unternehmen

Datenschutzbeauftragte

Kleinere Unternehmen wurden durch die Änderung der §§ 4d und 4f BDSG zwar formal entlastet, indem die Schwelle der mit der Datenverarbeitung betrauten Personen von vier auf neun heraufgesetzt wurde. Gleichzeitig wurde vom Arbeitnehmerbegriff abgewichen und es werden nun sämtliche mit der Verarbeitung betraute Personen einbezogen. D. h., dass sowohl der Geschäftsführer, als auch Auszubildende, Volontäre und Praktikanten im Gegensatz zur bisherigen Fassung zu berücksichtigen sind. Diese Änderung ist insofern zu begrüßen, als die Form des Beschäftigungsverhältnisses im Hinblick auf den Schutzbedarf irrelevant ist.

Unternehmen, die nach der bisher geltenden Fassung einen Datenschutzbeauftragten zu berufen hatten, haben nun die Wahl, diesen freiwillig weiterzubeschäftigen (wobei dessen Prüfungskompetenzen nun vertraglich zu regeln sind, da die §§ 4f und 4g BDSG auf diesen nicht mehr anwendbar sind), oder abzuberufen. Um nicht im Falle der Abberufung die Verarbeitungsverfahren melden zu müssen, wurden die Grenzen zu den Personenzahlen in gleicher Weise angepasst.

Eine echte Entlastung dürfte mit dieser Regelung nicht verbunden sein. Es ist zwar die Verpflichtung zur Bestellung eines Datenschutzbeauftragten und damit die interne Kontrollinstanz entfallen. Entgegen einer oft anzutreffenden Meinung ist es aber nicht so, dass die entsprechenden Betriebe nun ganz von den Datenschutzvorschriften befreit sind. Vielmehr hat die Unternehmensleitung selbst oder wie das Gesetz es formuliert „auf andere Weise" sicherzustellen, das diese Vorschriften eingehalten werden. Das heißt, das entsprechendes Fachwissen nun an anderer Stelle, z. B. in der Geschäftsleitung vorhanden sein muss.

Zur Abberufung eines betrieblichen Datenschutzbeauftragten siehe Bundesarbeitsgericht vom 13.03.2007 (9 AZR 612/05).

Eine weitere wesentliche Änderung ist, dass der Datenschutzbeauftragte nun ausdrücklich den gleichen Rechten und Pflichten unterliegt wie die verantwortliche Stelle. Dies macht die Bestellung eines externen Datenschutzbeauftragten auch bei Berufsgruppen mit besonderen Geheimhaltungspflichten (Ärzte, Rechtsanwälte) unproblematisch, da der Datenschutzbeauftragte dort das gleiche Zeugnisverweigerungsrecht hat, eine Beschlagnahme seiner Unterlagen in gleicher Weise ausgeschlossen ist und er den selben strafrechtlichen Konsequenzen im Falle des Geheimnisverrats unterliegt wie die verantwortliche Stelle selbst.

Bedauerlicherweise wurde es bei der Einfügung des § 203 Abs. 2 a) StGB versäumt in Absatz 3 auch die Mitarbeiter des Datenschutzbeauftragten einzubeziehen und damit den Mitarbeitern eines Rechtsanwaltes oder Arztes gleichzustellen. Hier besteht also nach Nachbesserungsbedarf.

Beratungsanspruch

Mit den Änderungen der §§ 4g und 38 des Bundesdatenschutzgesetzes ist nun rechtlich fixiert worden, was bisherige Praxis vertrauensvoller Zusammenarbeit zwischen betrieblichem Datenschutzbeauftragten und Aufsichtsbehörde war: Haben sich bisher die betriebliche Datenschutzbeauftragte in Zweifelsfragen an die Aufsichtsbehörden gewandt und diese auch anlassunabhängig Unternehmen, betriebliche Datenschutzbeauftragte und Verbände über datenschutzrechtliche Frage beraten, so haben die betrieblichen Datenschutzbeauftragten nun gegenüber der Aufsichtsbehörde einen gesetzlich abgesicherten Beratungsanspruch und die Aufsichtsbehörde eine entsprechende Verpflichtung.
Diese Klarstellung ist zu begrüßen und mag dazu führen, Hemmschwellen bei der Inanspruchnahme der Aufsichtsbehörde zu reduzieren.

Auswirkungen für den Betroffenen

Nachdem das Bundesdatenschutzgesetz seinerzeit als Reflex auf die technische Entwicklung und die damit einhergehenden neuen Möglichkeiten der Verarbeitung und Auswertung personenbezogener Daten entstanden ist, um weiterhin ein ausreichendes Datenschutzniveau zu garantieren, dient jetzt die zunehmende automatisierte Verarbeitung personenbezogener Daten in Klein- und Kleinstbetrieben als Grund, hier sowohl auf einen Datenschutzbeauftragten, als auch auf die Meldepflicht entsprechender Verfahren zu verzichten.
Dies stellt einen Paradigmenwechsel zu Lasten des Bürgers und Betroffenen dar. Stand die Rechtsetzung im Bereich des Datenschutzes bisher stets im Dienste des Bürgers mit dem Ziel den Einsatz neuer Techniken in für den Datenschutz vertretbare Bahnen zu lenken, dient nun die zunehmende Verbreitung der Datenverarbeitung als Argument zur Beschränkung ihrer Kontrolle. Diese Entwicklung werden wir im Rahmen unserer Aufsichtstätigkeit beobachten und, sofern Defizite für die Betroffenen festzustellen sind, für die bisherige Herangehensweise werben.

Neue Orientierungshilfen 4

Empfehlungen für den datenschutzgerechten Einsatz von Ratsinformationssystemen

In einer Vielzahl niedersächsischer Kommunen werden automatisierte Rats- oder Kreistagsinformationssysteme eingesetzt, die es der Verwaltung ermöglichen, den kommunalen Sitzungsdienst effizient zu steuern. Gleichzeitig haben die ehrenamtlichen Mandatsträger sowie die Bürgerinnen und Bürger die Gelegenheit, sich zeitnah über die in den kommunalen Gremien zur Beratung oder Beschlussfassung anstehenden Themen zu informieren. Hierdurch wird die Transparenz der Entscheidungen erhöht. Dies ist insbesondere für die Bürgerinnen und Bürger von großem Interesse, da sie gerade auf kommunaler Ebene von Entscheidungen unmittelbar berührt sind. Die Mandatsträger werden durch umfangreiche Recherche- und Archivfunktionen bei ihrer Arbeit unterstützt.

Die Vertraulichkeit und Integrität der in den Rats- und Kreistagsinformationssystemen verarbeiteten personenbezogenen Daten müssen aber jederzeit gewahrt bleiben.

Beim Landesbeauftragten eingehende Anfragen haben gezeigt, dass vielfach Unsicherheiten über eine datenschutzgerechte Ausgestaltung und Anwendung der Rats- und Kreistagsinformationssysteme bestehen, insoweit hat sich die Notwendigkeit ergeben, entsprechende Handreichungen hierfür herauszugeben. Dies ist im Jahr 2006 durch die Veröffentlichung (im Internetangebot des Landesbeauftragten) von Empfehlungen für den datenschutzgerechten Einsatz von Ratsinformationssystemen geschehen. Diese Empfehlungen sollen den Verwaltungen sowie Mandatsträgern eine Hilfestellung bei der konkreten Ausgestaltung und Anwendung der Rats- und Kreistagsinformationssysteme liefern.

Aufgabe der Datenschutzbeauftragten bleibt es weiterhin, den Einsatz derartiger Systeme sowohl bei ihrer Planung als auch im konkreten Einsatz zu beobachten, um das Recht auf informationelle Selbstbestimmung möglicher Betroffener vor denkbaren Beeinträchtigungen zu bewahren.

Empfehlungen für den datenschutzgerechten Einsatz von Ratsinformationssystemen, Seite 2:

„II. Chancen und Risiken

Der Einsatz automatisierter Rats- und Kreistagsinformationssysteme steigert ohne Zweifel die Effizienz der Aufgabenerledigung der kommunalen Verwaltungen in der Vor- und Nachbereitung der Sitzungen."

„Da jedoch die modernen Informations- und Kommunikationstechniken vielfältige Möglichkeiten bieten, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten, kann sich durch eine unzulässige Veröffentlichung im Internet und mangelnde Datensicherheit der in den Ratsinformationssystemen verarbeiteten und gespeicherten personenbezogenen Daten eine Gefährdung des Rechts auf informationelle Selbstbestimmung der Betroffenen ergeben."

Die Empfehlungen sind zu finden unter:
www.lfd.niedersachsen.de/
Themen/Kommunales/Ratsinformationssysteme

Orientierungshilfe zum Datenschutz für kommunale Mandatsträgerinnen und Mandatsträger

Zusammen mit dem Präsidenten des Niedersächsischen Städte- und Gemeindebundes, Herrn Rainer Timmermann habe ich im Oktober 2006 eine Orientierungshilfe zum Datenschutz für kommunale Mandatsträgerinnen und Mandatsträger herausgegeben.

Die Orientierungshilfe dient dazu, alle Kommunalpolitiker gleich zu Beginn ihrer Amtszeit über die wesentlichen Bestimmungen des Datenschutzes im Rahmen ihrer Mandatstätigkeit zu informieren.

Sie wurde an alle niedersächsischen Kommunen versandt und ist auf reges Interesse gestoßen. Sie wurde an die neu gewählten Mitglieder der Räte, der Kreistage und der Regionsversammlung verteilt und ist selbstverständlich auch im Internet abrufbar.

Um die Orientierungshilfe für den täglichen Einsatz leicht handhabbar zu gestalten, sind typische Fragen und Problemstellungen bei der kommunalen Mandats-

Die Orientierungshilfe ist zu finden unter:
www.lfd.niedersachsen.de/
Aktuelles/Pressemitteilungen/Orientierungshilfe zum Datenschutz für kommunale Mandatsträger

tätigkeit in Form von „häufig gestellten Fragen, den so genannten FAQ, behandelt. Diese sind im Anhang zu diesem Bericht abgedruckt.

Die Orientierungshilfe ist zu finden unter:
www.lfd.niedersachsen.de/
Service-Angebote/Empfehlungen
Recht/Datenschutz bei Dokumentenmanagementsystemen

Datenschutz bei Dokumentenmanagementsystemen (DMS) – Orientierungshilfe

Die „Orientierungshilfe Dokumentenmanagementsysteme“ ist von einer Arbeitsgruppe des Arbeitskreises eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet worden und von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in der Sitzung am 16./17. März 2006 zustimmend zur Kenntnis genommen worden.

Unter dem klassischen DMS im engeren Sinn sind solche Lösungen zu verstehen, die ursprünglich aus der Notwendigkeit entstanden sind, Instrumente und Verfahren für die Verwaltung der enorm wachsenden Dokumentenbestände zur Verfügung zu stellen. Hierzu zählt man Ablagesysteme zur Verwaltung der Dokumente im Lebenszyklus vor der Langzeitaufbewahrung. Wesentliche Eigenschaften sind visualisierte Ordnungsstrukturen sowie Kennzeichen zur Indizierung und Suchtechnologien. So gekennzeichnete Dokumente sind über mehr Informationsfelder recherchierbar, als sie ein Dateisystem zur Verfügung stellt. Beim DMS stehen beliebige Felder zur Verfügung wie beispielsweise Aktenzeichen, Eingangsdatum, Bearbeiter etc.

Unter einem DMS im weiteren Sinn werden verschiedene Systemkategorien und deren Zusammenspiel verstanden wie Dokumentenmanagement im engeren Sinn, Bürokommunikation, Scannen, Vorgangssteuerung (Workflow) und elektronische Aufbewahrung bis zum Übergang in Archivsysteme. Diese unterschiedlichen Komponenten sind in starkem Maße voneinander abhängig, der Einsatz einer Komponente ist im Allgemeinen nicht ohne den Zugriff auf andere Komponenten sinnvoll. Alle Module haben gemeinsam, dass unterschiedliche Arten von Dokumenten – gescannte Papierorginale als Scann-Datei, Faxeingänge, Dateien aus Büroanwendungen, E-Mails, Multimediaobjekte usw. – datenbankgestützt verwaltet werden. Der Einsatz von Datenbanken erlaubt die Handhabung großer Informationsmengen und einen direkten Zugriff auf einzelne Dokumente und Dokumentengruppen. In diesem Zusammenhang ist zum Beispiel der Bereich Erfassung, Darstellung und Ausgabe von gescannten Dokumenten (Imaging) unter dem Gesichtspunkt zu betrachten, dass es sich hierbei nur um eine spezielle Art von Dokumenten handelt.

Die Orientierungshilfe stellt die datenschutzrechtlichen und technischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur von DMS als Basiskomponente des eGovernment vor.

Sie will dazu beitragen, dass bei dem Einsatz eines DMS die Anforderungen von Datenschutz und Datensicherheit im Blick bleiben und praktische Hinweise dafür geben, wie diese Anforderungen in datenschutzgerechte und datenschutzfreundliche Anwendungen umgesetzt werden können.

Die präventive Überwachung der Telekommunikation … 5

… gemäß § 33a des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG)

Ein Bürger aus Niedersachsen hatte sich im Februar 2004 mit einer Verfassungsbeschwerde an das Bundesverfassungsgericht in Karlsruhe mit dem Ziel gewandt, die präventive Telekommunikationsüberwachung gemäß § 33a Nds. SOG für verfassungswidrig erklären zu lassen. Das Bundesverfassungsgericht hatte auch dem niedersächsischen Landesbeauftragten Gelegenheit zur Stellungnahme gegeben. Mit Schriftsatz vom 19. August 2004 hat der Landesbeauftragte die Position des Klägers gegenüber dem Bundesverfassungsgericht unterstützt.

www.lfd.niedersachsen.de/Themen/Innere Sicherheit/TK-Überwachung

Mit Entscheidung vom 27. Juli 2005 hat das Bundesverfassungsgerichts die Bestimmungen über die präventive Telekommunikationsüberwachung im Niedersächsischen Polizeigesetz für nichtig erklärt. Es hat unmissverständlich in Erinnerung gerufen, dass das Grundgesetz der Ausdehnung der polizeilichen Befugnisse in den Bereich der so genannten vorbeugenden Verbrechensbekämpfung und Straftatenverhütung deutliche Grenzen setzt.

1 BvR 668/04

Das Bundesverfassungsgericht führt in den Gründen aus, dass die polizeilichen Eingriffs- und Informationserhebungsbefugnisse in den letzten Jahren immer weiter in das Vorfeld von Straftaten oder konkreten Gefahrenlagen verlagert worden seien, wobei die Tatbestandsvoraussetzungen gleichzeitig immer unbestimmter und unklarer geworden seien. Eine Grenze zu den besonderen Befugnissen der Geheimdienste sei kaum noch zu erkennen. In der Praxis seien diese Befugnisse zudem vielfach zu reinen Verdachtsschöpfungsinstrumenten verwandelt worden und widersprächen damit dem Grundsatz der Unschuldsvermutung. In diese Entwicklung gehöre insbesondere die Befugnis zur präventiven Überwachung der Telekommunikation, mit der eine kaum eingrenzbare Zahl von Betroffenen unter den Generalverdacht künftig möglicher Straftaten gestellt werden kann.

In dieser Entscheidung hat das Bundesverfassungsgericht die tragenden Gründe seiner Entscheidungen vom 3. März 2004 zur akustischen Wohnraumüberwachung, dem so genannten Großen Lauschangriff, und zur präventiven Telekommunikationsüberwachung durch das Zollkriminalamt konsequent weiterentwickelt.

1 BvR 2378/98
1 BvF 3/92

Das Gericht hat hierzu ausgeführt, dass das Recht auf informationelle Selbstbestimmung zwar hinter die speziellere Gewährleistung aus Art. 10 GG zurücktritt, soweit die Schutzbereiche sich überschneiden; das Gleiche gelte auch für die Gewährleistung der freien Meinungsäußerung aus Art. 5 Abs. 1 GG, soweit der Eingriff in der staatlichen Wahrnehmung und gegebenenfalls Verarbeitung der per Telekommunikation geäußerten Meinungen liege.

Das Gericht hat jedoch unabhängig davon seinen Prüfungen in allen diesen Entscheidungen das Recht auf informationelle Selbstbestimmung, das den Einzelnen davor schützt, dass er durch den Umgang mit seinen personenbezogenen Informationen in seinem Persönlichkeitsrecht beeinträchtigt wird, als tragendes Prinzip zugrunde gelegt. Insbesondere aus der Unantastbarkeit der in Art. 1 Abs. 1 GG geschützten Würde des Menschen, die nach allen Entscheidungen einen elementaren Bestandteil des Rechts auf informationelle Selbstbestimmung bildet, hat das Bundesverfassungsgericht wiederum einen unantastbaren Kernbereich privater Lebensgestaltung abgeleitet, der jedem staatlichen Zugriff entzogen ist.

Der Kernbereich privater Lebensgestaltung ist jedem staatlichen Zugriff entzogen.

Hieraus folgt zwingend, dass sich die Folgerungen und Forderungen des Bundesverfassungsgerichts, insbesondere hinsichtlich der Beachtung eines unantastbaren Kernbereichs persönlicher Lebensgestaltung, nicht nur auf die in den drei Verfahren angegriffenen Einzelbestimmungen, sondern auf **alle** staatlichen Eingriffe in das Recht auf informationelle Selbstbestimmung beziehen.

Dass dabei verdeckte Datenerhebungen, bei denen Betroffene von sich aus keine Vorkehrungen gegen ein Eindringen in den unantastbaren Kernbereich persönlicher Lebensgestaltung und die Aufnahme entsprechender Informationen treffen oder sich dagegen auf andere Weise schützen können, besonders kritisch zu sehen sind, hat das Gericht deutlich gemacht: Es führt hierzu aus, dass ein verdeckter Informationseingriff eine besondere Intensität aufweise, weil die Betroffenen den Überwachungsmaßnahmen in einer Situation vermeintlicher Vertraulichkeit ausgesetzt werden; Eingriffe dieser Art würden darüber hinaus hohe Risiken für die Rechte der Betroffenen auch deshalb in sich bergen, weil diese gegen die Maßnahmen frühestens dann mit rechtlichen Mitteln vorgehen könnten, wenn sie bereits vollzogen sind, und dies auch nur, wenn sie darüber informiert würden oder auf andere Weise Kenntnis erlangten.

1 BvR 1550/03

Diese Auffassung hat das Bundesverfassungsgericht in seiner Entscheidung vom 13. Juni 2007 zur Verfassungsmäßigkeit der automatisierten Abfrage so genannter Kontostammdaten gemäß § 93 Abgabenordnung erneut bekräftigt.

Daneben legt das Bundesverfassungsgericht besondere Anforderungen für die Formulierung der gesetzlichen Eingriffsnormen in den Fällen fest, in denen Informationseingriffe im Präventivbereich stattfinden, also zur Vorsorge für die Verfolgung und die Verhütung von Straftaten vorgenommen werden; durch die strikte Beachtung des rechtstaatlichen Gebots der Normenbestimmtheit und Normenklarheit müsse sichergestellt werden, dass der betroffene Bürger sich auf mögliche belastende Maßnahmen einstellen kann, dass die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet und dass die Gerichte die Rechtskontrolle durchführen können. Bei der Vorverlagerung des Eingriffs in eine Phase, in der sich die Konturen eines Straftatbestandes noch nicht abzeichnen, bestehe das Risiko, dass der Eingriff an ein nur durch relativ diffuse Anhaltspunkte für mögliche Straftaten gekennzeichnetes, in der Bedeutung der beobachteten Einzelheiten noch schwer fassbares und unterschiedlich deutbares Geschehen anknüpfe.

Insbesondere bei verdeckten Datenerhebungen im präventiven Bereich müssen Gesetze bestimmt und klar sein,…

…damit sich mögliche Betroffene auf belastende Maßnahmen einstellen können und Gerichte die Maßnahme kontrollieren können…

…und es müssen handlungsbegrenzende Tatbestandselemente im Gesetz enthalten sein…

Sehe der Gesetzgeber in solchen Situationen Grundrechtseingriffe vor, so habe er die den Anlass bildenden Straftaten sowie die Anforderungen an Tatsachen, die auf die künftige Begehung hindeuten, so bestimmt zu umschreiben, dass das im Bereich der Vorfeldermittlung besonders hohe Risiko einer Fehlprognose gleichwohl verfassungsrechtlich noch hinnehmbar sei. Die Norm müsse handlungsbegrenzende Tatbestandselemente enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffe, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten sei.

…die einen vergleichbaren Standard an Vorhersehbarkeit und Kontrollierbarkeit schaffen, wie dies für überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist.

Es genüge nicht die auf Tatsachen gegründete, nicht näher konkretisierte Möglichkeit, dass jemand irgendwann in Zukunft Straftaten von erheblicher Bedeutung begehen werde.

Eine derart weite Ermächtigung werde dem Bestimmtheitsgebot nicht gerecht. Die Unbestimmtheit und das damit einhergehende Risiko der Fehlprognose werde nicht durch die Ausrichtung auf „Straftaten von erheblicher Bedeutung“ vermindert. Dieses Tatbestandsmerkmal biete keine Anhaltspunkte dafür, wann ein Verhalten auf die künftige Begehung solcher Straftaten hindeute. Die vom Gesetz in Bezug genommenen Straftatbestände seien in diesem Stadium, in dem der künftige Geschehensablauf noch offen sei, ohnehin nur wenig geeignet, den maßgeblichen Sachverhalt so einzugrenzen, dass er Indizien für eine zukünftige Straftatenbegehung biete. Darüber hinaus sei die Bezugnahme auf die Begehung von „Straftaten von erheblicher Bedeutung“ selbst in Teilen nicht hinreichend bestimmt.

Auf Wunsch der Mitglieder des Innenausschusses des Niedersächsischen Landtages hat der Landesbeauftragte in einem umfangreichen Schreiben im Dezember 2005 dem Ausschuss dargelegt, welche Auswirkungen die Entscheidungen des Bundesverfassungsgerichts zum sogen. Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung durch das Zollkriminalamt sowie zur präventiven Telekommunikationsüberwachung gemäß § 33a Nds. SOG auf niedersächsische Gesetzesregelungen haben.

Die Landesregierung hat am 29. Mai 2007 einen Gesetzentwurf zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung vorgelegt, mit dem die verfassungsgerichtlichen Vorgaben umgesetzt werden sollen.

LT-Drs. 15/3810

1 BvR 2378/98, Rd.-Nr. 303:
„Dies widerspricht dem verfassungsrechtlichen Anliegen der Gewährung effektiven Rechtsschutzes zum Zwecke der Abwehr von Beeinträchtigungen der hier in Rede stehenden Grundrechte."

1 BvR 668/04, Rd.-Nr. 163:
„Bestehen im konkreten Fall tatsächliche Anhaltspunkte für die Annahme, dass eine Telekommunikationsüberwachung Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben."

Allerdings sieht der Gesetzentwurf auch vor, dass ein Betroffener erst dann über einen gegen ihn gerichteten Einsatz von Vertrauenspersonen oder verdeckten Ermittlern zu unterrichten ist, wenn dadurch ein weiterer Einsatz dieser Personen nicht (mehr) gefährdet ist.
In der Anhörung durch den Ausschuss für Inneres und Sport des Niedersächsischen Landtags in seiner Sitzung am 19.06.2007 habe ich darauf hingewiesen, dass diese Regelung der Rechtsprechung des Bundesverfassungsgerichts widerspricht und deshalb gestrichen werden sollte.
Weiterhin soll nach dem Entwurf eine präventiven Telekommunikationsüberwachung zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person nur dann unzulässig sein, wenn davon auszugehen ist, dass sie **ausschließlich** eine Kommunikation erfasst, die als „höchstpersönlich dem Kernbereich privater Lebensgestaltung zuzurechnen ist".
Das Bundesverfassungsgericht hat hierzu jedoch die Vorgabe gemacht, dass eine Telekommunikationsüberwachung bereits dann unzulässig ist und unterbleiben muss, wenn im konkreten Fall tatsächliche Anhaltspunkte für die Annahme bestehen, dass sie **auch** Inhalte erfasst, die zu diesem Kernbereich zählen.
Ich habe in der Anhörung vor dem Ausschuss für Inneres und Sport auf die Verfassungswidrigkeit der beabsichtigten Regelung hingewiesen.
Ich hoffe, dass der Niedersächsische Landtag eine verfassungsrechtlich konsequente Lösung finden wird.

Arbeitnehmerdatenschutzgesetz 6

Eine unendliche Geschichte

Die seit vielen Jahren erhobenen Forderungen der Datenschutzbeauftragten an die Bundesregierung hinsichtlich einer gesetzlichen Implementierung bereichsspezifischer Vorschriften zum Arbeitnehmerdatenschutz blieben bisher ohne Erfolg. Angesichts stetig wachsender technischer Möglichkeiten muss jedoch klar geregelt werden, welche Daten Unternehmen über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen.

Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis sind vielfältig bedroht, zum Beispiel durch

- die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,
- die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutz der EG-Datenschutzrichtlinie gilt,
- die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,
- die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die Achtung des Grundrechts auf informationelle Selbstbestimmung der Arbeitnehmerinnen und Arbeitnehmer zählt ebenso zu guten und fairen Arbeitsbedingungen wie Chancengleichheit oder gerechte Bezahlung. Beschäftigtendatenschutz erhöht zudem die Motivation, trägt und fördert die Arbeitszufriedenheit und bedeutet damit einen nicht zu unterschätzenden Standortvorteil.
Den von der Bertelsmann Stiftung unter der Projektbezeichnung „Agenda Moderne Regulierung“ vorgelegten Diskussionsentwurf eines Arbeitsvertragsgesetzes (ArbVG), Verfasser sind die Professoren Dr. Henssler und Dr. Preis (beide Universität zu Köln), hat die vom sog. „Düsseldorfer Kreis“ eingerichtete Arbeitsgruppe „Beschäftigtendatenschutz“ zum Anlass genommen, im März 2007 erneut eine Initiative zur Aufnahme von Vorschriften zum Arbeitnehmerdatenschutz in ein ArbVG zu starten.
Ich unterstütze diese Initiative ausdrücklich und hoffe, dass die Bundesregierung den wiederholten Appell zur gesetzlichen Regelung des Arbeitnehmerdatenschutzes endlich aufgreift.

Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 in Erfurt:

„Die Konferenz fordert die Bundesregierung auf, sich für einen hohen gemeinsamen Mindeststandard des Arbeitnehmerdatenschutzes in Europa einzusetzen und in Deutschland zeitnah einen entsprechenden Gesetzentwurf vorzulegen.“

7 Völlige Unabhängigkeit?

Vertragsverletzungsverfahren der EU-Kommission gegen die Bundesrepublik Deutschland

Seit dem letzten Tätigkeitsbericht im Jahre 2003–2004 hat sich hinsichtlich der Rechtsstellung der Datenschutzkontrollstellen viel ereignet:
Am 5. Juli 2005 hat die Europäische Kommission ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland gemäß Artikel 226 des Vertrages zur Gründung der Europäischen Gemeinschaft (EG-Vertrag) wegen Verstoßes gegen die Richtlinie 95/46/EG (EG-Datenschutzrichtlinie) eingeleitet. Die Kommission begründet in Ihrer Stellungnahme vom 12. Dezember 2006 ihre Rechtsauffassung wie folgt:

Die Bundesrepublik Deutschland habe gegen ihre Verpflichtung aus Artikel 28 Abs. 1 Satz 2 der EG-Datenschutzrichtlinie verstoßen, indem sie die für die Überwachung der Datenverarbeitung im nicht-öffentlichen Bereich zuständigen Kontrollstellen in den 16 deutschen Ländern einer staatlichen Aufsicht unterwerfe. Damit werde die Vorgabe einer „völligen Unabhängigkeit" der Datenschutz-Aufsichtsbehörden fehlerhaft umgesetzt. Die Mitgliedstaaten seien verpflichtet, Regelungen zu treffen, die sowohl eine institutionelle, funktionelle als auch materielle Unabhängigkeit der Aufsichtsbehörden gewährleisten. Diese dürften

- keiner anderen Staatsgewalt untergeordnet sein (institutionelle Unabhängigkeit),
- in Bezug auf Inhalt und Umfang ihrer Tätigkeit keinerlei Weisungen unterliegen (funktionelle Unabhängigkeit),
- müssen selbständig über einen eigenen Haushalt verfügen (materielle Unabhängigkeit).

Richtlinie 95/46/EG, Artikel 28 – Kontrollstelle

(1) Die Mitgliedstaaten sehen vor, daß eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen. Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

Die Regierung der Bundesrepublik Deutschland widerspricht dieser Darlegung. Sie hält an ihrer wiederholt vertretenen Ansicht fest, dass die Organisation der Datenschutzkontrollstellen in Deutschland, unabhängig davon, wo die Aufgabenbereiche angesiedelt sind, der EG-Datenschutzrichtlinie entspreche und die Datenschutzbeauftragten ihre Aufgaben in völliger Unabhängigkeit wahrnehmen würden. Detailliert wird dies in der Mitteilung der Regierung der Bundesrepublik Deutschland an die Kommission vom 13. Februar 2007 begründet.
Allerdings konnte die Stellungnahme wohl nicht überzeugen, denn Mitte Juli 2007 hat die Kommission beschlossen, den Europäischen Gerichtshof mit der Angelegenheit zu befassen.
Während des Verlaufs der Diskussion wurde die in Niedersachsen zum 1. Januar 2006 vorgenommene Aufgabenverlagerung der Kontrolle über die Durchführung des Datenschutzes im nicht-öffentlichen Bereich nach dem Bundesdatenschutzgesetz (BDSG) auf das Niedersächsische Ministerium für Inneres und Sport rückgängig gemacht. Seit dem 1. Februar 2007 ist der Niedersächsische Landesbeauftragte für den Datenschutz wieder für diesen Aufgabenbereich zuständig (Beschluss der Niedersächsischen Landesregierung vom 19. Dezember 2006, Nds. MBl. 2007, S. 108).
Vor dem Hintergrund dieser Auseinandersetzung erwägt die Kommission, die Bestimmungen über die Rechtstellung der Datenschutzbeauftragten grundsätzlich zu überarbeiten und hierbei auch die materielle Mindestausstattung der Datenschutzbeauftragten zu präzisieren.
Es ist zu hoffen, dass das Verfahren zu einer datenschutzfreundlicheren Lösung führen wird.

Videoüberwachung, Webcams und kein Ende…

8

„Kann man denn nicht einmal unbeobachtet tanken und im Tankstellenshop eine Kleinigkeit einkaufen?“ So, oder ähnlich lauten die Anfragen an die Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich in den letzten Jahren. Diese Anfragen, persönliche Erfahrungen der Mitarbeiter und die Auswertung verschiedener Kontrollen waren dann die Beweggründe zur Durchführung anlassunabhängiger Kontrollen bei fünf Tankstellen in Niedersachsen. Die Auswahl erfolgte nach dem Zufallsprinzip; es traf Tankstellen aus Hannover, Braunschweig, Osnabrück, Oldenburg und Göttingen. Immer handelte es sich um Tankstellen, die von großen Mineralölfirmen gepachtet waren. Diese unterstützten nur in einem Fall ihre Tankstelle im Kontrollverfahren. Ein anderer Pächter wandte sich zur Erlangung von Hilfe an den Fachverband Tankstellengewerbe, der schließlich mit mir Kontakt aufnahm.

Eine Erkenntnis dieser Kontrolle war, dass Tankstellenpächter auf Grund ihres Pachtvertrages mehr oder weniger verpflichtet sind, ihre Tankstelle zu überwachen. Bis auf den einen Fall, bei dem der Mineralölkonzern sogar den externen Datenschutzbeauftragten stellt, werden die Pächter mit diesem Verfahren allein gelassen, auch dann, wenn eine solche Unterstützung ausdrücklich angefordert wird. Rein rechtlich sind die Mineralölkonzerne mit dieser Ablehnung auf der sicheren Seite, da verantwortliche Stelle für das Verfahren Videoüberwachung immer der Pächter ist. Ob dies auch moralisch vertretbar ist, sei dahingestellt.
Ergebnis der Kontrolle nach § 38 Bundesdatenschutzgesetz (BDSG) war, dass alle Tankstellen sowohl den Zapfsäulenbereich, als auch Teile des Shops überwachten. Waren Kameras überwiegend auf die Mitarbeiter ausgerichtet, was meist im Kassenbereich der Fall ist, haben die Pächter dies nach entsprechender Belehrung schnell abgestellt. Gelegentlich waren auch die erforderlichen Hinweisschilder nicht oder nicht an den richtigen Stellen installiert. Auch die gesetzlich erforderliche Verfahrensbeschreibung war meist nicht vorhanden, aus der der vor Beginn der Überwachung festzulegende Zweck der Überwachung zu entnehmen ist. Insgesamt war die Zusammenarbeit mit den Pächtern in diesem Kontrollverfahren jedoch kooperativ und vertrauensvoll. Zusammenfassend lässt sich feststellen, dass viele Fehler bei besserer Rechtskenntnis nicht begangen worden wären. Hier ist wohl eine bessere Information seitens der Verbände und eigentlich auch durch die verpachtenden Mineralölkonzerne gefragt. Meine Mitarbeiter wollen diesen Kontakt in der Zukunft ausweiten.
Auch Webcams haben in den vergangenen zwei Jahren immer wieder Anlass zu Überprüfungen gegeben. Insbesondere Hotels, Restaurants, Kaufhäuser und in letzter Zeit verstärkt Werbegemeinschaften einzelner Städte gehen immer mehr dazu über, ihre Internet-Auftritte durch solche Webcam-Übertragungen attraktiver zu gestalten und vorhandene Angebote zu visualisieren. Solange die Webcam-Bilder Personen nicht erkennen lassen, verletzt dies keine datenschutz-

Weiterführende Informationen:

Alle Hinweise zur Videoüberwachung durch private Stellen sind dem Faltblatt „Achtung Kamera!“ zu entnehmen, das der Berliner Beauftragte für Datenschutz und Informationsfreiheit, die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und der Landesbeauftragte für den Datenschutz Niedersachsen herausgegeben haben. Es ist über die Geschäftsstelle des Landsbeauftragten für den Datenschutz Niedersachsen, ~~Brühlstr. 9, 30169~~ Hannover zu beziehen.

Außerdem bietet der Niedersächsische Landesbeauftragte unter **www.lfd.niedersachsen.de/** Themen/Videoüberwachung die Informationen des Faltblattes im Web an.

Prinzenstr. 5, 30159

rechtlichen Belange. Gleiches gilt, wenn die Betroffenen damit einverstanden sind und diese Selbstdarstellung sogar ausdrücklich wünschen.
Das Recht des Einzelnen auf informationelle Selbstbestimmung ist aber spätestens dann berührt, wenn Personen erkennbar werden, die in die damit verbundene öffentliche Verbreitung und Zurschaustellung eben nicht eingewilligt haben, und ihnen – schlimmer noch – häufig überhaupt nicht bewusst ist, dass sie per Kamera beobachtet werden.

Webcams auch an der Autobahn?

Nein, auch wenn man fast den Eindruck haben könnte:
Auf dem 33 km langen Teilstück der Autobahn A 7 zwischen dem Autobahndreieck Walsrode und der Anschlussstelle Soltau-Ost befinden sich an insgesamt 94 Masten Videokameras (49 in Fahrtrichtung Hannover und 45 in Fahrtrichtung Hamburg). Die Kameras sind mit Infrarotscheinwerfern ausgerüstet und werden daher auch bei schlechten Sichtverhältnissen oder nachts, also 24 Stunden täglich, eingesetzt. Sie sind darüber hinaus schwenk- und zoombar. Die Bilder werden auf einem Ringspeicher gespeichert und erst nach 24 Stunden automatisch überschrieben.
Auf Anfrage teilte mir die Niedersächsische Landesbehörde für Straßenbau und Verkehr mit, dass die Kameras Teil einer dort installierten Verkehrsbeeinflussungsanlage sind und der Verkehrsüberwachung auf diesem Streckenabschnitt dienen, um u. a. bei geeigneten Verkehrslagen die Standspur als dritte Fahrspur freigeben zu können bzw. wieder zu sperren. Im laufenden Verkehr sind die aufgenommenen Bilder zu undeutlich, um Fahrzeuginsassen oder Kennzeichen erkennen zu können. Daher ist das Verfahren grundsätzlich datenschutzrechtlich unbedenklich. An dieser Einschätzung ändert auch die Tatsache nichts, dass insgesamt 4 Stellen (Verkehrsmanagementzentrale Niedersachsen, Fernmeldemeisterei Hannover, Autobahnmeisterei Fallingbostel, Autobahnpolizei Bad Fallingbostel) auf die Kameras zugreifen können.
Bei einer Überprüfung der Anlage habe ich jedoch festgestellt, dass der Schwenkbereich der Kameras so weitgehend ist, dass auch die in diesem Streckenabschnitt vorhandenen Parkplätze problemlos überwacht werden können. Die Leistungsfähigkeit der Kameras ist derart groß, dass die Kennzeichen der dort haltenden Fahrzeuge deutlich lesbar und die Gesichter der Fahrzeuginsassen selbst durch die Frontscheiben erkennbar sind. Außerhalb der Fahrzeuge stehende Personen werden nahezu in „Passbildqualität“ abgebildet.
Als Teil der installierten Verkehrsbeeinflussungsanlage ist eine Überwachung der Parkplätze sicher nicht erforderlich.
Ist es denkbar, dass einige der beteiligten Stellen andere Motive für die Überwachung der Parkplätze haben (Beobachtung illegaler Abfallentsorgung oder von Straftaten, an Stelle der Benutzung der Toiletten …)?
Ich habe auf meine entsprechende Nachfrage nach Sinn und Zweck und den entsprechenden Rechtsgrundlagen bis Redaktionsschluss die mündliche Auskunft bekommen, dass nunmehr der Sichtbereich der Kameras so eingeschränkt worden sei, dass die Parkplätze nicht mehr überwacht werden können.

Weiterführende Informationen:

Rechtsgrundlage zur Videoüberwachung durch öffentliche Stellen zur Ausübung des so genannten Hausrechts (also außerhalb speziell geregelter Befugnisse z. B. nach dem Gesetz über die öffentliche Sicherheit und Ordnung) ist § 25a Niedersächsisches Datenschutzgesetz.

Hierzu bietet der Niedersächsische Landesbeauftragte unter

www.lfd.niedersachsen.de/ Datenschutzrecht/Nds. Recht eine ausführliche Kommentierung an.

Die elektronische Gesundheitskarte (eGK) 9

In meinem XVII. Tätigkeitsbericht (Seite 28) wurde über die Planungen zur Einführung der Elektronischen Gesundheitskarte (eGK) berichtet.

Wie in dem Bericht näher ausgeführt, werden auf der Karte in einer ersten Stufe neben den persönlichen Angaben wie Name, Krankenversichertennummer, Krankenkasse auch elektronische Rezepte und Notfalldaten gespeichert . Weitere Daten sollen im Laufe der Zeit hinzukommen wie der elektronische Arztbrief und als „Krönung“ die elektronische Patientenakte.
Während das elektronische Rezept als Pflichtbestandteil vorgesehen ist, werden die anderen Anwendungen nur mit Einwilligung des Versicherten aufgenommen. Auch soll der Versicherte innerhalb der einzelnen Anwendungen, also z. B. der elektronischen Patientenakte, den Zugriff auf die Daten steuern können, indem er z. B. dem einen Facharzt den Zugriff auf bestimmte Teile der Patientenakte verweigert, ihn aber einem anderen Facharzt einräumt.
Die elektronische Patientenakte stellt also ein höchst komplexes Vorhaben dar. Nicht überraschend ist daher, dass der Termin der ursprünglich geplanten Einführung, der 1. Januar 2006, längst überschritten ist.
Immerhin sind die Pilotprojekte, in denen die Karte unter annähernd realen Bedingungen getestet werden soll, vorangekommen. Zu den sieben Modellregionen in Deutschland gehört das „eHealthProjekt Wolfsburg“. Unter meiner Beteiligung wurde das Verfahren für die Auswahl der Ärzte, Krankenhäuser, Apotheken und Versicherten, die die Funktionsfähigkeit der Karte erproben sollen, entwickelt. Die Auswahl der Ärzte, Krankenhäuser und Apotheken ist beendet. Der schwierigere Teil der Gewinnung von 10.000 Versicherten soll bis zum Sommer 2007 abgeschlossen sein, so dass anschließend der Test beginnen kann.
Ich werde, ebenso wie meine Kollegen im Bund und in den Ländern, die Einführung der elektronischen Gesundheitskarte in Arbeitsgruppen und vor Ort in der Modellregion Wolfsburg begleiten.

ELENA-Verfahren (ehemals JobCard-Verfahren) 10

In meinem XVII. Tätigkeitsbericht (Seite 26) habe ich das JobCard-Verfahren, jetzt ELENA-Verfahren (Elektronischer Einkommensnachweis), vorgestellt.

Trotz der Umbenennung ist die Grundstruktur erhalten geblieben. Bei dem ELENA-Verfahren handelt es sich um ein System zur Speicherung von Verdienst-, Entgelt- und Arbeitsbescheinigungsdaten (z. B. Zeiten der Beschäftigung), die für sozialrechtliche Zwecke, aber auch für zwei gerichtliche Verfahren (Prozesskostenhilfe und Unterhaltsverfahren) benötigt werden.

Nach der Konzeption sollen die Daten in der zentralen Speicherstelle (ZSS) gespeichert werden, die sie den Sozialleistungsträgern und Gerichten auf Abruf zur Verfügung stellt.

Die Daten werden in der ZSS nicht unter dem Namen des Bürgers, sondern unter einer verschlüsselten Identifikationsnummer vorgehalten. Ein Abruf setzt voraus, dass sowohl der Leistungsberechtigte als auch der Mitarbeiter der Behörde bzw. des Gerichts seine jeweilige Signaturkarte einsetzt.

Wie bereits in meinem XVII. Tätigkeitsbericht ausgeführt, wirft das Verfahren verfassungsrechtliche Fragen auf, etwa, ob es sich um eine unzulässige Vorratsdatenspeicherung handelt, weil es für einen großen Teil der Bevölkerung niemals erforderlich sein wird, die gespeicherten Daten zu nutzen.

Der vom Bundeswirtschaftsministerium im November 2006 vorgelegte Entwurf eines ELENA-Gestzes greift dieses Problem auf und legt die Zwecke, für die die Daten gespeichert werden dürfen, präzise fest, so dass den Forderungen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15.12.1983 nach meiner Auffassung Genüge getan ist. 1 BvR 209/83

Weitere datenschutzrechtliche Fragen sind noch ungelöst. Die 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 7. bis 9. März 2007 hat zu ihnen Stellung genommen, etwa, in welchen Ausnahmefällen eine Entschlüsselung der Daten ohne Vorlage der Signaturkarte des Leistungsberechtigten zulässig sein soll.

Über die weitere Entwicklung werde ich in meinem Internetangebot berichten.

11 Melderegister und Zensusvorbereitungsgesetz

Meldewesen

Sachstand: In enger Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz Niedersachsen wurde das niedersächsische Melderecht an die rahmenrechtlichen Vorgaben des novellierten Melderechtsrahmengesetzes angepasst. Auch das elektronische Rückmeldeverfahren zwischen den Meldebehörden ist seit dem 1. Januar 2007 verbindlich eingeführt.
Durch die Föderalismusreform wurde der Übergang des Meldewesens in die ausschließliche Gesetzgebungskompetenz des Bundes beschlossen. Die Fortentwicklung des Meldewesen wird auch zukünftig von höchstem Interesse für die Datenschutzbeauftragten sein. Zur Prüfung der Bedingungen für eine Fortentwicklung des Meldewesens wurde durch das Bundesministerium des Innern (BMI) eine Arbeitsgruppe eingesetzt, deren Bericht nunmehr vorliegt und dessen Ergebnisse den Datenschutzbeauftragten des Bundes und der Länder vorgestellt wurden. Auf Empfehlung der Arbeitsgruppe sollen ein Bundesmeldegesetz erlassen und ein Bundesmelderegister eingerichtet werden.

Ausblick: Die Entwicklung des Bundesmeldegesetzes und -registers wird von Seiten der Datenschutzbeauftragten kritisch begleitet werden, um durch konstruktive Mitarbeit bei der Entwicklung der künftigen Strukturen eine möglichst datenschutzgerechte Gestaltung zu erreichen.

Zensusvorbereitungsgesetz

Ausführliche Erläuterungen zum EU-weiten Zensus 2011 enthält das gemeinsame Internetangebot der Statisitschen Ämter des Bundes und der Länder (http://www.statistik-portal.de/Statistik-Portal/zensus/).

Durch die Kommission der Europäischen Gemeinschaften (EU-Kommission) wird derzeit eine Verordnung vorbereitet, die die Durchführung eines EU-weiten Zensus für das Jahr 2011 in allen EU-Mitgliedstaaten verbindlich vorschreiben wird. Ein Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Volks- und Wohnungszählungen wurde auch bereits vorgelegt. Die Mitgliedstaaten sollen so verpflichtet werden, Grunddaten ihrer Bevölkerung und der Gebäude und Wohnungen nach einheitlichen Definitionen an die Europäische Union (EU) zu liefern.

Die Bundesregierung hat durch Kabinettsbeschluss im August 2006 erklärt, sich an der EU-Volkszählung beteiligen zu wollen. Entsprechend befindet sich ein Vorbereitungsgesetz für die Durchführung des Zensus in Deutschland, zu dem sich die Datenschutzbeauftragten des Bundes und der Länder in einer gemeinsamen Stellungnahme bereits geäußert haben, im Abstimmungsverfahren der Bundesministerien. Die Beratungen des Zensusvorbereitungsgesetzes im Bundestag sind noch nicht abgeschlossen. Der Beschluss des Gesetzes wird voraussichtlich im Herbst 2007 erfolgen

Abweichend von der Volkszählung 1987 sollen die benötigten Daten nicht mehr durch eine Befragung aller Einwohner erhoben werden. Grundlage des Zensus ist vielmehr eine registergestützte Erhebung, bei der vor allem auf Daten der Melderegister und der Bundesagentur für Arbeit sowie auf Dateien zum Personalbestand der Öffentlichen Hand zurückgegriffen werden soll. Dazu kommen stichprobenartige Befragungen zur Sicherung der Datenqualität bei etwa 10 % der Bevölkerung und Befragungen der Verwaltung oder Bewohner von Gemeinschaftsunterkünften, Anstalten, Wohnheimen und ähnlichen Einrichtungen. Lediglich die Gebäude- und Wohnungseigentümer sollen noch postalisch befragt werden.

Durch die Durchführung des registergestützten Zensus soll die Belastung der Bevölkerung im Gegensatz zu der Volkszählung in den 80er Jahren möglichst gering gehalten werden. Der Gesetzgeber hat also aus den damaligen Auseinandersetzungen, die nicht zuletzt datenschutzrechtlicher Natur waren, Konsequenzen gezogen. Aufgabe der Datenschutzbeauftragten des Bundes und der Länder wird es nun sein, darauf zu achten, dass der Datenschutz und die Vorgaben des Volkszählungsurteils vom 15. Dezember 1983 eingehalten werden.

Elektronische Steuererklärung und steuerliche Identifikationsnummer 12

Elektronische Steuererklärung (ELSTER)

Seit Juni 2001 bietet die Finanzverwaltung bundesweit die elektronische Übermittlung von Steuererklärungen an. Für Lohnsteuer-Anmeldungen und Umsatzsteuer-Voranmeldungen ist die elektronische Übermittlung seit 2005, für Lohnsteuerbescheinigungen bereits seit 2004 verpflichtend.

Während in den ersten Jahren noch neben der elektronischen Fassung zusätzlich ein Exemplar der Steuererklärung in Papierform mit persönlicher Unterschrift versehen abzugeben war, soll nunmehr allein die elektronisch übermittelte Steuererklärung genügen. Die bisher gemäß § 87a Abs. 3 S. 2 Abgabenordnung (AO) für diese Form der Übermittlung vorgesehene qualifizierte elektronische Signatur nach dem Signaturgesetz (vgl. § 2 Nr. 3 SigG) hat der Gesetzgeber mit Verabschiedung des Jahressteuergesetzes 2007 durch Änderung des § 87a Abs. 6 AO und der Steuerdatenübermittlungsverordnung (StDÜV) dahingehend relativiert, dass nunmehr bis zum 31.12.2011 auch ein anderes sicheres Verfahren zur elektronischen Übermittlung zugelassen werden kann.

Für die elektronische Übermittlung wie für den Abruf steuerlicher Daten wird deshalb seitens der Finanzverwaltung ein einheitliches Authentifizierungsverfahren angeboten, das lediglich einer **einmaligen** Identifizierung und Registrierung des Nutzers bedarf. Das daraus erstellte Zertifikat wird in einer Datei auf dem eigenen PC oder einem sog. ELSTER-Stick (USB-Stick mit Kartenleser und Speicherchip) gespeichert. Dieses Zertifikat wird dann mit der elektronischen Steuererklärung versandt und ersetzt nach den Angaben der Finanzverwaltung die bisherige Unterschrift auf der Steuererklärung.

Steuererklärungen sind nach den geltenden Steuergesetzen grundsätzlich schriftlich und mit Unterschrift versehen bei den Finanzbehörden einzureichen (vgl. u. a. § 150 AO i. V. m. § 25 Einkommensteuergesetz, § 18 Umsatzsteuergesetz, § 14a Gewerbesteuergesetz).

Authentifizierung im Sinne des geänderten § 6 Abs. 1 StDÜV bedeutet im Falle der elektronischen Übermittlung einer Steuererklärung, dass diese nicht mehr wie bisher bei der Abgabe von körperlichen Steuererklärungen mit eigenhändiger Unterschrift versehen werden müssen, sondern die zuvor im Elster-Online-Portal elektronisch durchgeführte Identifikation der übermittelnden Person von der Finanzverwaltung als ausreichend angesehen wird. Dabei bleibt jedoch die Authentizität und die Integrität (Unversehrtheit) der übermittelten Steuererklärung und ihres Inhalts unberücksichtigt. Es ist also nicht sicher, dass die Steuererklärung tatsächlich von dem Steuerpflichtigen stammt und dass sie bei der Übermittlung nicht verändert wurde.

Entgegen der Auffassung der Finanzverwaltung weist das Authentisierungsverfahren systembedingt nicht die gleiche Sicherheit auf, die unter Verwendung einer qualifizierten elektronischen Signatur erreicht wird. Die qualifizierte elektronische Signatur im Sinne des SigG stellt ein elektronisches Siegel dar. Erst sie macht die übermittelte elektronische Steuererklärung mit einem mit eigenhändiger Unterschrift versehenen körperlichen Schriftstück vergleichbar.

Die rechtliche Qualität dieser Signatur bewirkt, dass die Angaben in der elektronisch übermittelten Steuererklärung dem betreffenden Steuerpflichtigen rechts-

wirksam zugerechnet werden können. Nur derjenige, der seine Steuererklärung mit einer qualifizierten digitalen Signatur versehen übermittelt, ist somit auch in der Lage nachzuweisen, dass ein unter falscher Nutzung der Authentifizierung elektronisch übermitteltes Dokument nicht von ihm selbst stammt.
Im Ergebnis führt der neue Weg in Streitfällen zu einer Umkehr der Beweislast zum Nachteil des Steuerpflichtigen.

§ 87a Abs. 3 und 6 AO Elektronische Kommunikation

(3) [1]Eine durch Gesetz für Anträge, Erklärungen oder Mitteilungen an die Finanzbehörden angeordnete Schriftform kann, soweit nicht durch Gesetz etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. [2]In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. [3]Die Signierung mit einem Pseudonym ist nicht zulässig.

(6) [1]Das Bundesministerium der Finanzen kann durch Rechtsverordnung mit Zustimmung des Bundesrates für die Fälle der Absätze 3 und 4 neben der qualifizierten elektronischen Signatur bis zum 31. Dezember 2011 auch ein anderes sicheres Verfahren zulassen, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. [2]Einer Zustimmung des Bundesrates bedarf es nicht, soweit Verbrauchsteuern mit Ausnahme der Biersteuer betroffen sind. [3]Die Verwendung des anderen sicheren Verfahrens ist zu evaluieren.

§ 1 StDÜV
(Stand lt. Verordnung vom 20.12.2006 – BGBl. I S. 3380)

Allgemeines

(1) Für das Besteuerungsverfahren erforderliche Daten mit Ausnahme solcher Daten, die für die Festsetzung von Verbrauchsteuern bestimmt sind, können durch Datenfernübertragung übermittelt werden (elektronische Übermittlung). Mit der elektronischen Übermittlung können Dritte beauftragt werden.

(2) Das Bundesministerium der Finanzen bestimmt in Abstimmung mit den obersten Finanzbehörden der Länder Art und Einschränkungen der elektronischen Übermittlung von Daten nach Absatz 1 Satz 1 durch ein im Bundessteuerblatt zu veröffentlichendes Schreiben. In diesem Rahmen bestimmte Anforderungen an die Sicherheit der elektronischen Übermittlung sind im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik festzulegen. Einer Abstimmung mit den obersten Finanzbehörden der Länder bedarf es nicht, soweit ausschließlich die Übermittlung von Daten an Bundesfinanzbehörden betroffen ist.

(3) Bei der elektronischen Übermittlung sind dem jeweiligen Stand der Technik entsprechende Verfahren einzusetzen, die die Authentizität, Vertraulichkeit und Integrität der Daten gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden.

(4) Die in dieser Verordnung genannten Pflichten der Programmhersteller sind ausschließlich öffentlich-rechtlicher Art.

§ 6 Abs. 1 StDÜV

Authentifizierung, Datenübermittlung im Auftrag

(1) Abweichend von § 87a Abs. 3 Satz 2 der Abgabenordnung ist bei der elektronischen Übermittlung keine qualifizierte elektronische Signatur erforderlich, wenn ein anderes Verfahren eingesetzt wird, welches den Datenübermittler authentifiziert und die in § 1 Abs. 3 S. 1 bestimmten Anforderungen an die Gewährleistung der Authentizität und Integrität der Daten erfüllt.

Steuerliche Identifikationsnummer

Sachstand: In meinem letzten Tätigkeitsbericht (Seite 20) hatte ich bereits die Auswirkungen aufgezeigt, die die Einführung einer solchen steuerlichen Identifikationsnummer haben könnte. So wird mit dem Bundeszentralamt für Steuern (BZSt) erstmals eine zentrale Stelle über die Grunddaten (z. B. Familiennamen, frühere Namen, Vornamen, Geburtsdaten, Geburtsorte, Anschriften) aller 80 Millionen Bundesbürger verfügen. Sobald diese Datenbestände aufgebaut sind, steht zu befürchten, dass hierauf auch außerhalb der Finanzverwaltung Begehrlichkeiten geweckt werden und sehr bald Überlegungen angestellt werden, diese Datenbestände auch für andere Zwecke zu nutzen.

Mit Verordnung vom 28. November 2006 (BGBl I S. 2726 ff.) sind nun die Einführung und Vergabe steuerlicher Identifikationsnummern zum 1. Juli 2007 und deren Übermittlung von den Meldebehörden an das BZSt geregelt worden.

Vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und den Landesbeauftragten für den Datenschutz wurde das Verordnungsverfahren intensiv begleitet und dabei insbesondere die Schaffung einer entsprechenden Rechtsgrundlage zur Einführung eines „Vorläufigen Bearbeitungsmerkmals“ in § 139b Abs. 6 Abgabenordnung bis zur endgültigen Vergabe der steuerlichen Identifikationsnummer ereicht.

Weiterhin wurde die Einbindung des Bundesamtes für Sicherheit in der Informationstechnik im Hinblick auf die Sicherheit und Funktionsfähigkeit des Datenübermittlungsverfahrens sichergestellt.

Bei der Übermittlung von Daten der Meldebehörden an das BZSt auf Datenträgern ist nunmehr vorgesehen, diese zumindest mit einer fortgeschrittenen Signatur i. S. v. § 2 Abs. Nr. 2 SigG zu versehen und nach dem Stand der Technik zu verschlüsseln.

§ 2 Nrn. 1–3 Signaturgesetz (SigG, in der aktuellen Fassung)

§ 2 SigG Begriffsbestimmungen

Im Sinne dieses Gesetzes sind

1. „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,
2. „fortgeschrittene elektronische Signaturen“ elektronische Signaturen nach Nummer 1, die

a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

3. „qualifizierte elektronische Signaturen" elektronische Signaturen nach Nummer 2, die
a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
b) mit einer sicheren Signaturerstellungseinheit erzeugt werden,

Ausblick: Die weitere Entwicklung und Durchführung der Datenübermittlungen und des Aufbaus und Abgleichs der Datenbestände in den Meldebehörden und im BZSt werden von Seiten der Datenschutzbeauftragten weiterhin begleitet. Insbesondere ist darauf zu achten, dass die Datenbestände und die vergebenen Identifikationsnummern nur für die gesetzlich vorbestimmte Identifikation im Besteuerungsverfahren Verwendung finden.

Auszug aus dem „Jahressteuergesetz 2007 (JStG 2007)" vom 13.12. 2006 (BGBl I S. 2878)

Der geänderte § 139 b Abs. 6 Abgabenordnung lautet nun wie folgt:

(6) Zum Zwecke der erstmaligen Zuteilung der Identifikationsnummer übermitteln die Meldebehörden dem Bundeszentralamt für Steuern für jeden in ihrem Zuständigkeitsbereich mit alleiniger Wohnung oder Hauptwohnung im Melderegister registrierten Einwohner folgende Daten:

1. Familienname,
2. frühere Namen,
3. Vornamen,
4. Doktorgrad,
5. Ordensnamen/Künstlernamen,
6. Tag und Ort der Geburt,
7. Geschlecht,
8. gegenwärtige Anschrift der alleinigen Wohnung oder der Hauptwohnung.

Hierzu haben die Meldebehörden jedem in ihrem Zuständigkeitsbereich mit alleiniger Wohnung oder Hauptwohnung registrierten Einwohner ein Vorläufiges Bearbeitungsmerkmal zu vergeben. Dieses übermitteln sie zusammen mit den Daten nach Satz 1 an das Bundeszentralamt für Steuern. Die Übermittlung der Daten nach Satz 1 erfolgt ab dem Zeitpunkt der Einführung des Identifikationsmerkmals, der durch Rechtsverordnung des Bundesministeriums der Finanzen auf Grund von Artikel 97 § 5 Satz 1 des Einführungsgesetzes zur Abgabenordnung bestimmt wird. Das Bundeszentralamt für Steuern teilt der zuständigen Meldebehörde die dem Steuerpflichtigen zugeteilte Identifikationsnummer zur Speicherung im Melderegister unter Angabe des Vorläufigen Bearbeitungsmerkmals mit und löscht das Vorläufige Bearbeitungsmerkmal anschließend.

Zusammenarbeit mit der Finanzverwaltung 13

Beratungsbesuche in niedersächsischen Finanzämtern

Zu meiner Tätigkeit nach § 22 NDSG gehört auch die Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften bei den Behörden der Finanzverwaltung.

Im Rahmen dieser Tätigkeit habe ich Beratungsbesuche bei den niedersächsischen Finanzämtern durchgeführt. Bei diesen Beratungsbesuchen sind unter Beteiligung der Oberfinanzdirektion Hannover Datenschutzfragen aus der Praxis der Finanzverwaltung und des Besteuerungsverfahrens erörtert sowie Handlungsempfehlungen zur Sicherung von Betroffenenrechten und zu organisatorischen Maßnahmen gegeben worden.

Zur Vorbereitung dieser Beratungsbesuche habe ich dem jeweiligen Finanzamt einen „Erhebungsbogen“ zugesandt, in dem sowohl Grundinformationen zu örtlichen und organisatorischen Gegebenheiten angefordert, als auch materiellrechtliche Fragestellungen aufgegriffen wurden. Die Ergebnisse der durchgeführten Beratungsbesuche wurden schriftlich fixiert und den betroffenen Finanzämtern und der Oberfinanzdirektion übermittelt.

Sowohl die zuvor übersandten Erhebungsbögen als auch die nachträglich übermittelten Ergebnisvermerke wurden von den Finanzbehörden genutzt, noch genauer datenschutzrechtliche Regelungen zu beachten und ggf. organisatorische Maßnahmen zur besseren Wahrung des Datenschutzes zu ergreifen.

Die durchgeführten Beratungsbesuche trugen insbesondere auch zur intensiveren Zusammenarbeit zwischen dem Landesbeauftragten für den Datenschutz und den niedersächsischen Finanzbehörden, insbesondere der Oberfinanzdirektion, auf dem Gebiet des Datenschutzes bei.

Die Beratungsbesuche werden bei weiteren Finanzämtern fortgesetzt.

Schulungen zum Datenschutz in der niedersächsischen Finanzverwaltung

Den niedersächsischen Finanzbehörden konnten zahlreiche Schulungen zum Datenschutz angeboten werden, die eine gute Resonanz gefunden haben.

So haben Mitarbeiter meiner Dienststelle an der Niedersächsischen Fachhochschule für Verwaltung und Rechtspflege (Fachbereich Steuerverwaltung) in Rinteln und an der Finanzschule in Bad Eilsen (beides zusammen jetzt Steuerakademie Niedersachsen) wiederholt zum Thema Datenschutz unterrichtet.

Weiterhin wurden jeweils entsprechend angepasste datenschutzrechtliche Schulungen für die Führungskräfte, die Geschäftsstellenleitungen der Finanzämter (als behördliche Datenschutzbeauftragte), für die Mitarbeiter dieser Geschäftsstellen und für die Personalvertretungen der niedersächsischen Finanzverwaltung angeboten und erfolgreich durchgeführt.

Eine Fortführung dieser Angebote ist geplant.

Gläserne Bankkonten? Kontenabrufverfahren nach §§ 93 Absatz 7 und 8, 93b Abgabenordnung

14

Durch Artikel 2 des „Gesetzes zur Förderung der Steuerehrlichkeit“ vom 23. Dezember 2003 (BGBl I S. 2928 ff.) wurde zum 1. April 2005 für die Finanzbehörden die Möglichkeit zur Durchführung eines Kontenabrufverfahrens im Besteuerungsverfahren geschaffen. Das Bundesministerium der Finanzen (BMF) hat bereits am 10. März 2005 in einem Anwendungserlaß zur Abgabenordnung (AEAO) Regelungen zur Durchführung dieses Verfahrens getroffen.
Nach § 93 Abs. 7 Abgabenordnung (AO) kann die einzelne Finanzbehörde über das Bundeszentralamt für Steuern (BZSt) so genannte Kontenstammdaten von Bürgern abrufen, wenn dies für das Besteuerungsverfahren erforderlich ist und ein Auskunftsersuchen an den Bürger nicht zum Ziele geführt hat oder keinen Erfolg verspricht. Hierbei teilt das BZSt auf Antrag die folgenden Bestandsdaten zu Konten- und Depotverbindungen mit:

- Nummer eines Kontos oder Depots,
- Tag der Errichtung und Tag der Auflösung des Kontos oder Depots,
- der Name des Inhabers und eines Verfügungsberechtigten, bei natürlichen Personen auch der Tag der Geburt,
- der Name und die Anschrift eines abweichend wirtschaftlich Berechtigten.

Kontenbestände und -bewegungen werden nicht mitgeteilt.
Anders als ursprünglich vom Gesetzgeber beabsichtigt, werden diese Kontenabrufe in der Praxis im Wesentlichen nicht im Steuerfestsetzungs- oder im Steuererhebungsverfahren, sondern überwiegend im Rahmen der Zwangsvollstreckung durchgeführt. Nach § 93 Abs. 8 AO können auch andere Behörden, z. B. Sozialbehörden, über das BZSt diese Daten abrufen.
Im Rahmen von Beratungsbesuchen bei den niedersächsischen Finanzämtern habe ich festgestellt, dass die betroffenen Steuerpflichtigen vor dem Abruf häufig nicht über diese (neue) Möglichkeit durch die Finanzbehörde informiert wurden, obwohl diese Information nur unterbleiben darf, wenn der Zweck des Abrufverfahrens sonst gefährdet würde. Auch fehlte es regelmäßig an der notwendigen Dokumentation der erforderlichen Ermessensausübung, die zu dem jeweiligen Kontenabruf geführt hat. Ich habe die Finanzbehörden im Rahmen meiner Ergebnismitteilungen auf diese festgestellten Mängel hingewiesen. Soweit möglich, wurden daraufhin die erforderlichen Dokumentationen nachgeholt und die Steuerbürger über die durchgeführten Kontenabrufe informiert.
Bei den Beratungsbesuchen habe ich ebenfalls festgestellt, dass nur vereinzelt Kontenabrufe nach § 93 Abs. 8 AO durchgeführt worden sind. So sind seit Einführung des Verfahrens zum 1. April 2005 bis zum 31. Dezember 2006 in Niedersachsen insgesamt 30 Kontenabrufe auf Ersuchen anderer Behörden veranlasst worden.
Durch intensive Zusammenarbeit in einer Projektgruppe mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den übrigen Landesbeauftragten für den Datenschutz wurde ein Mustervordruck zur Dokumentation der Entscheidungsgründe für einen Kontenabruf nach § 93 Abs. 7 AO

erstellt und dem Bundesministerium der Finanzen sowie der niedersächsischen Finanzverwaltung zur Verfügung gestellt.

1 BvR 1550/03

Mit Beschluß vom 13. Juni 2007 hat das Bundesverfassungsgericht (BVerfG) entschieden, dass der § 93 Abs. 8 AO, der auch anderen Behörden außerhalb der Finanzverwaltung die Möglichkeit zum Ersuchen eines Kontenabrufs über die Finanzbehörde einräumt, gegen das Gebot der Normenklarheit und -bestimmtheit verstößt, da er den Kreis der Behörden, die ein solches Ersuchen stellen können und die Aufgaben, denen diese Ersuche dienen sollen, nicht hinreichend bestimmt.

Weiterhin hat das Gericht betont, dass Kontenabrufe nur im Rahmen konkreter Verdachtsmomente erlaubt sind, aber nicht routinemäßig oder ‚ins Blaue hinein' erfolgen dürfen. Das BVerfG stellte klar, dass eine Sammlung der dem Grundrechtsschutz unterliegenden persönlichen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht mit dem Grundgesetz vereinbar ist. Die Informationsbeschaffung muß verhältnismäßig sein und ist auf das zu diesem Zweck Erforderliche zu beschränken.

§ 93 Abs. 7 und 8 Abgabenordnung (in der aktuell gültigen Fassung)

Auskunftspflicht der Beteiligten und anderer Personen

(7) Die Finanzbehörde kann bei den Kreditinstituten über das Bundeszentralamt für Steuern einzelne Daten aus den nach § 93b Abs. 1 zu führenden Dateien abrufen, wenn dies zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht.

(8) Knüpft ein anderes Gesetz an Begriffe des Einkommensteuergesetzes an, soll die Finanzbehörde auf Ersuchen der für die Anwendung des anderen Gesetzes zuständigen Behörde oder eines Gerichtes über das Bundeszentralamt für Steuern bei den Kreditinstituten einzelne Daten aus den nach § 93b Abs. 1 zu führenden Dateien abrufen und der ersuchenden Behörde oder dem ersuchenden Gericht mitteilen, wenn in dem Ersuchen versichert wurde, dass eigene Ermittlungen nicht zum Ziele geführt haben oder keinen Erfolg versprechen.

Ausblick auf geplante Gesetzesvorhaben

Im Rahmen der geplanten Einführung eines Unternehmensteuerreformgesetzes 2008 sollen auch die §§ 93 Abs. 7 und 8 AO geändert werden. Der neue § 93 Abs. 7 AO soll im Zuge der Einführung einer Abgeltungssteuer auf private Zinsen und private Veräußerungsgewinne ab 1. Januar 2009 die Befugnis der Finanzbehörden, Kontenabrufe zu veranlassen, auf die Fälle beschränken, in denen auch nach Einführung der Abgeltungsteuer noch die Erforderlichkeit besteht, Konten und Depots von Steuerbürgern zu ermitteln.

Der neue § 93 Abs. 8 AO knüpft nun nicht mehr wie bisher an Begriffe des Einkommensteuergesetzes an, sondern enthält in Satz 1 eine Aufzählung außersteuerlicher Zwecke, zu denen ein Kontenabrufersuchen anderer Behörden zulässig ist. Weiterhin ist vorgesehen, dass nicht mehr die Finanzbehörde das Ersuchen der zuständigen Behörde an das BZSt weiterleitet, sondern die zuständige Behörde das Kontenabrufersuchen unmittelbar an das BZSt richtet. Auch in diesen Fällen ist Voraussetzung, dass ein Auskunftsersuchen an den Steuerbürger nicht zum Ziele geführt hat oder keinen Erfolg verspricht.

Datenschutz in Schulen 15

Ein E-Learning-Projekt mit dem Computerzentrum des Niedersächsischen Landesamtes für Lehrerbildung und Schulentwicklung (NiLS)

Aufgrund der Neuorganisation des gesamten Schulbereichs durch die Einführung der Eigenverantwortlichen Schule und der damit verbundenen Änderungen des Niedersächsischen Schulgesetzes (NSchG), hat die Verunsicherung hinsichtlich der geltenden datenschutzrechtlichen Regelungen sowohl auf Seiten der Beschäftigten der Schulen als auch auf Seiten der Schülerinnen und Schüler sowie deren Erziehungsberechtigten stark zugenommen. Vermehrt erreichen mich Anfragen der Schulen, der Lehrkräfte und der Eltern. Oftmals ist auf Seiten der Schulen nicht einmal bekannt, dass auch sie gem. § 8 Niedersächsisches Datenschutzgesetz (NDSG) verpflichtet sind, einen eigenen Datenschutzbeauftragten zu bestellen.

Die Fragen, die an mich herangetragen werden, betreffen häufig die veränderten rechtlichen Grundlagen, die neuen Verfahrensregelungen in den Schulen z. B. zur Lernstandsentwicklung oder der Meldung von Zeugnisnoten zur Evaluation der Schullaufbahnempfehlungen, die Internetpublikationen der Schulen, den Aufbau und Betrieb von Computernetzwerken und den Einsatz von Schulverwaltungssoftware.

Wegen der Bedeutung des Themas habe ich zusammen mit dem Niedersächsischen Landesamt für Lehrerbildung und Schulentwicklung (NiLS) das Projekt „Datenschutz in Schulen“ ins Leben gerufen.

Ziele des Projektes sind die Förderung eines datenschutzgerechten Umgangs mit personenbezogenen Daten der Lehrkräfte und der Schülerinnen und Schüler sowie ihrer Erziehungsberechtigten, die Unterstützung der Datenschutzbeauftragten, der Verwaltungsmitarbeiter und der Lehrkräfte der Schulen und nicht zuletzt auch die Information der Schülerinnen und Schüler sowie die Information ihrer Erziehungsberechtigten über ihre – auf den Datenschutz bezogenen – Rechte und Pflichten. Langfristig sollen alle Beteiligten für die Belange des Datenschutzes sensibilisiert werden.

Bei der Vermittlung des datenschutzrechtlichen Grundlagenwissens habe ich gemeinsam mit dem NiLS neue Wege beschritten. Mit Unterstützung des Niedersächsischen Kultusministeriums (MK) wurde eine Projektgruppe eingerichtet, die sich die Entwicklung und Erprobung von E-Learning-Modulen für eine internetgestützte Fortbildung zum Thema „Datenschutz in Schulen“ zum Ziel gesetzt hat. Vertreten in dieser Projektgruppe sind neben meiner Geschäftsstelle das MK und Praktiker aus den Schulen.

Durch die Nutzung internetgestützter Fortbildungstechniken soll mit vertretbarem personellen und finanziellen Aufwand für die Vermittlung grundlegender Bestimmungen und Verfahrensweisen des Datenschutzes in Schulen gesorgt und ein tragfähiges Unterstützungssystem geschaffen werden.

Die Arbeit der Projektgruppe ist mittlerweile soweit fortgeschritten, dass der internetgestützte Fortbildungskurs konzipiert, eine Kooperations- und Lernumgebung aufgebaut und die Online-Materialien entwickelt worden sind. Ein erster Pilotkurs zu Erprobung des erstellten Materials hat bereits stattgefunden und die Rückmeldungen der einzelnen Teilnehmer können durchweg als sehr positiv bezeichnet werden.

Anhand der Anregungen der Teilnehmer des Pilotkurses wurden die erstellten Online-Materialien mittlerweile nochmals überarbeitet und können seit Beginn der Sommerferien 2007 für die allgemeine Lehrerfortbildung in Niedersachsen eingesetzt werden. Darüber hinaus ist geplant, geeignete Themenbereiche auch als Internetbeitrag auf meiner Internetseite für die Allgemeinheit zur Verfügung zu stellen. Außerdem wird durch die Projektgruppe zurzeit geprüft, inwieweit es möglich ist, das Thema ‚Datenschutz in Schulen‘ auch in die Pflichtfortbildung von zukünftigen Schulleiterinnen und Schulerleitern sowie in den Aufgabenbereich der Schulinspektion einzufügen.

Weiterführende Informationen:

Die Online-Materialien sind auf der niedersächsischen Kooperations- und Lernplattform für Schule und Fortbildung (nline) veröffentlicht und können unter folgendem Link eingesehen werden:

www.nline.nibis.de/datenschutz/menue/nibis.phtml?menid=44

SCHWERPUNKT: technisch-organisatorischer

Selbstdatenschutz – auf dem Weg zur Bürgerpflicht

Die schöne neue Welt …

Während die Gruppe der 14- bis19-Jährigen mit über 95 % nahezu vollständig erschlossen ist und die über 60-Jährigen mit bisher 20 % noch das höchste Erschließungspotential bieten (Stand 12.2006), ist der Trend eindeutig:
Die regelmäßige Nutzung des Mediums Internet beeinflusst unseren Alltag zunehmend – und das in immer mehr privaten Lebensbereichen.
Stand früher die reine Informationsbeschaffung im Vordergrund, bestimmen mittlerweile zunehmend interaktive Angebote das Feld. Online-Banking, Internet-Shopping, die Teilnahme an Chats, Newsgroups und Gesprächsforen, E-Mail-Nutzung und zahllose weitere Dienste und Angebote werden für viele Bürger immer selbstverständlicher und vor allem – wohl auch unverzichtbarer.

… und ihre Schattenseiten

Beipiel Google: „Daten-Deal mit Pferdefuß"
Die in Deutschland derzeit beliebteste Suchmaschine im Internet, Google, ist nicht nur ein fleißiger Datensammler, um schnell und umfassend weltweite Fundstellen zu beliebigen Stichworten, Informationsfragmenten und Bildern zur Verfügung zu stellen. Der „Deal" mit den Daten verlangt auch eine Gegenleistung: Google sammelt auch Informationen der Benutzer und speichert sie 18 Monate lang. Dazu gibt es eine Verknüpfung mit dem persönlichem Cookie des Benutzerbrowsers. Gelegentlich werden sogar die angeklickten Links protokolliert. Die Browser-Toolbar schickt bei den erweiterten Funktionen die besuchten Webseiten an Google und „Google Desktop" gibt Datenfunde des eigenen Rechners preis, denn Google lagert den Inhalt jeder Datei, derer es mit der Desktop-Suchmaschine habhaft werden kann, auf seinen Servern. Daher sollte sich jeder

Dabei wandelt sich der bisher relativ anonyme Surfer mehr und mehr zum identifizierbaren Objekt so mancher Begierde. Er wird allenthalben zur Preisgabe persönlicher Informationen animiert und hinterlässt teils leichtfertig, teils notgedrungen – und oft genug auch ohne sein Wissen – eine für manch anderen durchaus interessante Datenspur.
Darüberhinaus setzt er sich mit seiner technischen Umgebung einer zunehmenden Gefährdung durch Angriffe von Dritten aus; Viren, Würmer und Trojaner verrichten ihre Dienste, „korrumpieren" die Systeme und sind in der Lage, sicher geglaubte persönlichste Daten auszuspähen.

Auf verlorenem Posten?

Während im beruflichen Arbeitsumfeld durch geschulte Administratoren ein relativ geschützter Internetzugang gewährleistet werden kann, ist der private Nutzer zu Hause oftmals überfordert. Schlecht vorkonfigurierte Softwareinstallationen, die darauf ausgerichtet sind, schnell einsatzfähig, aber nicht unbedingt sicher zu sein, sparsame oder unverständliche Bedienungsanleitungen und ein Wust von versteckten Funktionalitäten machen es oft – auch bei gutem Willen – schwer, den eigenen PC mit vertretbarem Aufwand ausreichend zu schützen.

Datenschutz

16

Gefahr erkannt …

Durch die zunehmende Bedrohungslage ist allerdings nicht nur das Recht auf informationelle Selbstbestimmung des Einzelnen gefährdet. Die Korrumpierung zahlreicher privater Systeme stellt gleichermaßen ein nicht zu unterschätzendes Sicherheitsrisiko für die gesamte Infrastruktur des Internetverkehrs dar.

Da auch erste Gerichtsurteile die Tendenz aufzeigen, Betreiber von nach allgemeinem Erkenntnisstand ungenügend abgesicherten Internetzugängen in die Störerhaftung zu nehmen, ist eines klar: Jeder Einzelne ist gefordert, nicht nur im Eigeninteresse, sondern auch aus der Verantwortung für Dritte, sich des Themas anzunehmen und entsprechende Vorsichtsmaßnahmen zu treffen!

Selbstdatenschutz wird zur Bürgerpflicht!

Infizierte PCs lassen sich mit krimineller Energie zu so genannten bot-Netzen organisieren, von denen aus zunehmend ferngesteuerte Angriffe auf Anbieter von Internetdiensten gestartet werden. Laut Meldung von heise-online vom 26.01.2007 steht bereits jeder 4. Internet-PC im Verdacht, auf diese Weise unfreiwillige Handlangerdienste zu leisten.

Auch ungenügend abgesicherte Funknetzwerke (WLANs) stellen für unsichtbare Eindringlinge ein beliebtes Sprungbrett dar, um unbemerkt und unter falscher Identität ihr Unwesen zu treiben.

… und gemeinsam gebannt!

Ich habe es mir im Rahmen meiner Öffentlichkeitsarbeit und Beratungstätigkeit zur Aufgabe gemacht, für diesen Bereich Hilfestellungen mit möglichst breitem Wirkungsgrad zu geben. Kooperationspartner verschiedenster Ebenen waren bereit, erste Schritte auf diesem Weg mitzugehen und so entstanden Produkte, die auf unterschiedlichste Weise Multiplikatoreffekte erzielen können:

- Zusammenarbeit mit den Volkshochschulen
  Gemeinsam mit dem Landesverband der Volkshochschulen Niedersachsen e. V. wurde ein **Grundkurs „Datensicherheit"** entwickelt, der sich an private Anwender sowie kleine Gewerbebetriebe richtet und Grundlagenkenntnisse in Datensicherheit und Datenschutz vermitteln soll. Das Themenspektrum reicht von der Absicherung des Betriebssystems, über Schutzmaßnahmen im Internet- und E-Mail-Verkehr bis zur Datenverschlüsselung. Der Kurs ist für 24 Unterrichtsstunden konzipiert, kann mit einer Prüfung abge-

überlegen, ob wirklich alle angebotenen Dienste genutzt werden sollten oder ob weniger sammelfreudige Alternativdienste oder auch der Verzicht in Frage kommt. Zudem bieten alle Browserprogramme z. B. Optionen zum Löschen von Cookies, besuchten Seiten etc. Auf diese Gefahren habe ich bereits in meinem XVI. Tätigkeitsbericht hingewiesen. (Auszug: http://cdl.niedersachsen.de/blob/images/C1384942_L20.pdf).

Weiterer Link:

http://de.wikipedia.org/wiki/Google#Datenschutz

schlossen werden und steht bundesweit allen Volkshochschulen zur Aufnahme in ihr Programmangebot zur Verfügung.

- Einbindung privater Initiativen
  Vor der Herausgabe meiner neuesten Veröffentlichung zum Thema „System- und Datensicherheit für Jedermann“ sollte deren Anwendertauglichkeit getestet werden. Mit der freundlichen Unterstützung der Initiative „hi-senior“ (ein Zusammenschluss interessierter und versierter PC- und Internetnutzer der 50+-Generation aus Hildesheim) erfuhr die **Publikation „Sicherheit in Funknetzwerken“** ihren letzten Schliff. Sie steht unter www.lfd.niedersachsen.de > Service-Angebote > Selbstdatenschutz zum Download bereit und ist nach „PC-Sicherheit für Einsteiger“ das zweite Werk in dieser Reihe.

- Kooperation mit den Profis
  Als interaktives Angebot für einen PC-Selbsttest wurde gemeinsam mit dem Heise Zeitschriften Verlag ein **Netzwerk-Check** entwickelt, der kostenlos online zur Verfügung steht. Dabei werden über eine Netzwerkverbindung zum aufrufenden Rechner dessen für den Internet-Verkehr möglicherweise geöffneten Anschlüsse geprüft (Port-Scan). Das Scan-Ergebnis wird aufgelistet, bewertet und zur Verfügung gestellt. Im Normalfall sollten die meisten Ports geschlossen sein. Werden verdächtige offene Anschlüsse erkannt, ergeben sich klare Handlungsempfehlungen zur Absicherung des getesteten Systems. Da der Anwender mit Bordmitteln nicht in der Lage ist, die Existenz derartiger Schlupflöcher aufzuspüren, stellt der unter www.lfd.niedersachsen.de > Service-Angebote > Selbstdatenschutz > Testangebote aufrufbare Service ein hilfreiches und häufig frequentiertes Mittel zur Abwehr möglicher Angriffsszenarien dar.

Ich hoffe, dass die Summe dieser Angebote sowohl zur Sensibilisierung aller Betroffenen führt, als auch deren Möglichkeiten zur aktiven Selbsthilfe stärkt. Gemeinsam sollte es gelingen, ein Stück weit mehr Sicherheit in diesem Bereich aufzubauen.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de
> Service-Angebote > Selbstdatenschutz

www.datenschutz.de
> Schlagwortsystem > Technik > Selbstdatenschutz
(Virtuelles Datenschutzbüro)

www.bsi-fuer-Buerger.de
(Bundesanstalt für Sicherheit in der Informationstechnik)

www.buerger-cert.de
(bietet kostenfreie aktuelle Warnmeldungen und Sicherheitshinweise per E-Mail)

Datenschutz im Rundfunk- und Telemedienrecht 17

Datenschutz im Rundfunkrecht

Rechtsgrundlagen, die datenschutzrechtliche Fragen aufwerfen, sind im Rundfunkstaatsvertrag bzw. im Rundfunkgebührenstaatsvertrag zu finden.

Nach wie vor ist das gegenwärtige System der Rundfunkgebührenerhebung datenschutzrechtlich kritisch zu betrachten. Die zur Feststellung der Gebührentatbestände erforderlichen Datenerhebungen und -verarbeitungen stehen im Missverhältnis zum Recht auf informationelle Selbstbestimmung der Rundfunkteilnehmer. Insbesondere die Übermittlungen aus dem Melderegister an die Landesrundfunkanstalten zum Abgleich bei der Feststellung der Gebührenpflicht sind sehr problematisch zu bewerten. Sie könnten gänzlich entfallen, wenn die öffentlich-rechtliche Rundfunkfinanzierung grundsätzlich überarbeitet werden würde. Statt der gegenwärtigen individuellen Gebühr würde eine von der Vorhaltung der Empfangsgeräte unabhängige Abgabe die Datenerhebung vollständig überflüssig machen.

Auch die im Jahre 2006 geführte Diskussion um die internetfähigen Computer als Rundfunkempfänger würde sich mit einem Systemwechsel erübrigen, bei der es darum ging, dass internetfähige Endgeräte, gleichgültig ob beruflich oder privat genutzt, ob Notebook, PC, Handy oder PDA-Taschencomputer, öffentlich rechtliche Rundfunksender über das Internet empfangen können (Internetradio) und damit als faktische Rundfunkempfänger die Gebührenpflicht auslösen.

Ebenso die Aufgaben der Rundfunkgebührenbeauftragten wären mit einem Systemwechsel der Finanzierung nicht mehr notwendig. Ihnen obliegt derzeit, Bürgerinnen und Bürger in ihren Haushalten und Büros aufzusuchen, um die Voraussetzungen für die individuelle Rundfunkgebührenpflicht festzustellen. Diese Tätigkeit erzeugt seit Jahren ein erhebliches Beschwerdeaufkommen bei uns und den Datenschutzbeauftragten der Rundfunkanstalten und erklärt auch teilweise, warum die umfangreichen Datenerhebungen nicht auf große Akzeptanz bei den Bürgern stoßen.

Aus diesen technischen und rechtlichen Gründen halte ich die grundlegende Überarbeitung des Finanzierungssystems für unausweichlich.

Datenschutzunfreundliche Gebührenbefreiung

Bei der Befreiung von der Rundfunkgebührenpflicht sind die Verfahren bisher sehr datenintensiv ausgestaltet gewesen.

Die GEZ ist Empfängerin zahlreicher Informationen, die für die Abwicklung der Gebührenbefreiung nicht erforderlich sind. Das trifft insbesondere auf Sozialdaten zu, wenn diese sehr zahlreich durch Vorlage des gesamten Bescheides über Arbeitslosengeld II vorgelegt worden sind. Dieser Personenkreis stellt den größten Anteil an Gebührenbefreiungsanträgen.

Sofern bei der Sozialbehörde Gebührenbefreiung beantragt wird, werden dort die Einkünfte und Vermögensverhältnisse aller im Haushalt lebenden Familien-

Der Rundfunkgebührenstaatsvertrag ist als Artikel 4 des Staatsvertrags über den Rundfunk im vereinten Deutschland vom 31.08.1991, zuletzt geändert durch den neunten Staatsvertrag zur Änderung rundfunkrechtlicher Staatsverträge vom 31.07./10.10.2006 verabschiedet worden. (Nds. GVBl. 1991, S. 311 (GVBl. 2007, S. 60))4

mitglieder erfasst. Wenn der Antrag auf Gebührenbefreiung Erfolg hat, gelangen die Unterlagen u. U. zur Gebühreneinzugszentrale (GEZ).
In Gesprächen zwischen Vertretern der Landesregierungen, den Datenschutzbeauftragten der Landesrundfunkanstalten und Vertretern der Datenschutzbeauftragten der Länder wurden Lösungen erörtert, um diese Verfahren zu vereinfachen und die Privatsphäre der Rundfunkteilnehmer besser zu schützen. Denkbar wäre eine datenreduzierte Bescheinigung, die nur die für die Befreiung erforderlichen Informationen enthält. Die GEZ hat bereits technische Vorschläge unterbreitet, die aus technischen und rechtlichen Gründen von der Bundesagentur für Arbeit bisher nicht mitgetragen wurden. Bis in das Jahr 2007 gab es noch keine bundesweit einheitliche Regelung, die von der Arbeitsagentur in datensparsame Formulare umgesetzt worden wäre. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten von Bund und Ländern befasst sich auch weiterhin mit dem Thema und bemüht sich um eine fachliche Beratung für eine bundesweit einheitliche datenschutzfreundliche Lösung.

GEZ

Im Berichtszeitraum sind wieder zahlreiche Anfragen und Beschwerden im Zusammenhang mit der Handhabung der Radio- und Fernsehgebühren durch die Rundfunkanstalten, die Rundfunkgebührenbeauftragten und die Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ in Köln) bei mir eingegangen. Meist geht es um die personenbezogenen Daten durch Wechsel der Wohnanschrift, des Familienstandes oder der Haushaltszugehörigkeit.
Im Grundsatz werden die Teilnehmerdaten an die GEZ, soweit für die Gebührenbearbeitung erforderlich, von den Rundfunkteilnehmern selbst durch Anmeldevordrucke mitgeteilt.
Zusätzlich dürfen aber die Meldebehörden der GEZ mitteilen, wenn eine volljährige Person zu- oder wegzieht oder verstirbt. Diese regelmäßige Datenübermittlung wurde rechtlich bewusst zugelassen, damit die öffentlich-rechtlichen Rundfunkanstalten die Rundfunkgebühren ordnungsgemäß einziehen können und damit die Finanzierung der öffentlich-rechtlichen Rundfunkversorgung der Bürger sichergestellt wird.
Letztlich ist es der GEZ erlaubt, zusätzlich den privatrechtlichen Adresshandel zu bemühen.
Die geschilderte Datenerhebungs- und Übermittlungspraxis und die auftretenden Datendifferenzen verursachen gelegentlich Missverständnisse. Insbesondere bei Namensänderungen oder wenn in einem Haushalt mehrere Volljährige mit unterschiedlichen Namen zusammenleben.
Die GEZ speichert und verarbeitet die Daten der Rundfunkteilnehmer ausschließlich zum Zweck des Gebühreneinzugs in ihrer Funktion als Gemeinschaftseinrichtung der öffentlich-rechtlichen Landesrundfunkanstalten der ARD und des ZDF (Zweites Deutschen Fernsehen) in deren Auftrag.

Systembruch

Der zusätzliche Verweis des § 8 Abs. 4 Rundfunkgebührenstaatsvertrag auf den § 28 Bundesdatenschutzgesetz (BDSG) eröffnet die Quellennutzung der Landesrundfunkanstalten und der beauftragten GEZ sowohl im öffentlichen wie im nicht öffentlichen Bereich. Dies stellt nach meiner Auffassung rechtssystematisch einen Bruch dar.

Rundfunk, also Radio und Fernsehen, ist aus verfassungsrechtlichen Gründen aus der Kontrollbefugnis der Landesdatenschutzbeauftragten ausgenommen. In diesem Bereich werden eigene Datenschutzbeauftragte für den Rundfunk tätig.

Die Einhaltung des Datenschutzes im Zusammenhang mit der Erhebung der Rundfunkgebühr wird durch den Staatsvertrag für Rundfunk und Telemedien und die Landesdatenschutzgesetze geregelt.
Nach § 2 Abs. 5 des Niedersächsischen Datenschutzgesetzes (NDSG) gilt für öffentlich-rechtliche Rundfunkanstalten das Recht des jeweiligen Sitzlandes.
Die Datenschutzaufsicht über die Tätigkeit der GEZ in Niedersachsen übt nach dem Rundfunkstaatsvertrag der Datenschutzbeauftragte des NDR in Hamburg aus. (Dessen Tätigkeitsbericht beinhaltet weitere Aussagen auf diesem Gebiet zur Entwicklung des Datenschutzes der Sendeanstalt und auch im Bereich der GEZ-Themen).
Petenten müssen deshalb letztlich von uns zuständigkeitshalber an den Datenschutzbeauftragten des NDR verwiesen werden.

NDR-Datenschutz
Der aktuelle Tätigkeitsbericht des Datenschutzbeauftragten des Norddeutschen Rundfunks (DSB NDR) für 2006 gibt Auskunft über die Schwerpunkte seiner Arbeit im Berichtszeitraum 1. Januar bis 31. Dezember 2006 unter www1.ndr.de/unternehmen/organisation/datenschutz

Tele- und Medienrecht

1. Trotz „täglicher Leiden“: Sichere E-Mails sind selten

Einer aktuellen Studie[1] zufolge besitzen 69 % der Bundesbürger bzw. 63 % der Bundesbürgerinnen ab 14 Jahren eine persönliche E-Mail-Adresse. 2004 lag die Quote noch bei 51, 2002 sogar erst bei 38 %[2]. Verstärkt wird dieser Trend dadurch, dass die Nutzung von E-Mail auch am Mobiltelefon in wenigen Jahren zum Massenmarkt werden dürfte[3].
Fast täglich erreichen uns Anfragen Betroffener, die durch den Mangel an verlässlichen Merkmalen verunsichert sind, ob ihr Mailverkehr richtig organisiert ist. Hauptursache ist meist die fehlende Authentizität der Nachrichten.
Tatsächlich sind E-Mails grundsätzlich potentiell unsicher. Diese zunächst vielleicht überraschende Aussage zu der inzwischen häufigsten Kommunikationsform neben dem Telefon erklärt sich schnell, wenn man vier wichtige Risiken betrachtet:

- Eine E-Mail kann ohne größeren Aufwand von jedermann gelesen werden (mangelnde Vertraulichkeit).
- Der Inhalt ist nicht fälschungssicher (mangelnde Integrität).
- Absender und Adressat sind beliebig manipulierbar (mangelnde Authentizität).
- Der Eingang beim Adressaten ist nicht nachweisbar (mangelnde Nichtabstreitbarkeit).

[1] Monatsumfrage BITKOM e.V. 25.07.2007 www.bitkom.org/47328_47322.aspx
[2] BITKOM e.V. 14.05.2007 www.bitkom.org/47328_45843.aspx
[3] Studie des Marktforschers Gartner vom Juli 2007 www.gartner.com

Diese Bewertung verdeutlicht auch die Ursachen für die enorm gestiegenen Zahlen für Schadsoftware und Werbeattacken. Spam-Mails[4], aber auch Phishing-Versuche mit dem Ziel des Identitätsdiebstahls mit einem Rekordaufkommen verursachen bei allen Benutzern einen hohen Leidensdruck und bei den IT-Betrieben hohe Kosten. Die weltweite Spamquote lag Ende 2006 bei 74 %, wie das britische E-Mail-Sicherheitsunternehmen MessageLabs berichtete. Andere Unternehmen kommen auf noch höhere Quoten. Das Prinzip der Vortäuschung falscher Absender rührt von der Tatsache, dass Mails nahezu kostenlos versandt werden können. Andere Schadsoftware (so genannte Malware) findet ebenso bevorzugt über den E-Mail-Weg ihre Opfer[5].
Konsequenterweise sollte dieses Medium E-Mail daher nicht bedenkenlos für schutzwürdige Inhalte genutzt werden. Allerdings gibt es auch sichere Alternativen, wie die E-Mail-Kommunikation durch technische Maßnahmen, wie z. B. einer Nachrichtenverschlüsselung, abgesichert werden kann.

[4] BSI-Studie, März 2005: Antispam-Strategien, unerwünschte E-Mails erkennen und abwehren www.bsi.de/literat/studien/antispam/antispam.pdf Allgemeine Informationen und Tipps gegen Spam: www.bsi-fuer-buerger.de/abzocker/05_06.htm

[5] Informationen und Hilfen zu Schadprogrammen: (Malware wie Computerviren, Würmer, Trojanische Pferde, Falschmeldungen/Hoaxes) www.bsi.de/av Kurzinformationen zu Spyware, Bot-Netze, Spam, Phishing, DoS-Attacken www.bsi-fuer-buerger.de/abzocker

Material zum Selbstdatenschutz

Näheres dazu wird auf unseren Webseiten www.lfd.niedersachsen.de unter Service-Angebote > Selbstdatenschutz > Downloads angeboten:
In der Reihe „System- und Datensicherheit für Jedermann, Material zum Selbstdatenschutz" haben wir zwei Teile herausgegeben:
Teil 1 **„PC-Sicherheit für Einsteiger"** und
Teil 2 **„Sicherheit in Funknetzwerken"**

Allgemein gilt:

Werden mit dieser (oder einer anderen) Technik personenbezogene Daten oder sonst vertraulich oder authentisch zu behandelnde Informationen übertragen, muss eine Risikoanalyse durchgeführt werden, innerhalb derer – unter Abwägung des Schutzbedarfs der Daten und deren möglicher Gefährdungen – verschiedene Sicherheitsmaßnahmen auf ihre Eignung zu prüfen sind. Dabei muss der Aufwand für die Maßnahmen unter Berücksichtigung des Standes der Technik in einem angemessenen Verhältnis zu dem angestrebten Zweck stehen. Wird ein verbleibendes Restrisiko als zu hoch und damit als nicht beherrschbar eingestuft, darf eine entsprechende Anwendung nicht zum produktiven Einsatz kommen.

Die Verantwortung für diesen „datenschutzkonformen" Betriebszustand obliegt stets dem Betreiber. Auch die Beauftragung eines Dienstleisters mit der Konzipierung, der Entwicklung oder dem Betrieb entlässt den Auftraggeber nicht aus der inhaltlich-fachlichen Verantwortlichkeit.

2. „Private Internetnutzung am Arbeitsplatz: Lösungsansätze für eine Trennung der privaten und dienstlichen Internetnutzung"

Unter diesem Titel haben wir 2006 mit einem Projekt Lösungsansätze untersucht.

Obwohl die Nutzung von Internet und E-Mail am Arbeitsplatz nicht mehr wegzudenken ist, wird deren private Nutzung noch immer stiefmütterlich behandelt. Aus Angst vor einer missbräuchlichen Nutzung oder ausufernden Kosten scheuen sich viele Arbeitgeber, den Mitarbeitern die elektronischen Kommunikations- und Informationsdienste für den privaten Gebrauch zu überlassen. Die Konsequenz: Internet und E-Mail dürfen und sollen weiterhin aus dienstlichem bzw. geschäftlichen Anlass genutzt werden, der private Gebrauch wird hingegen sanktioniert und ist tabu.

Eine Verbotsregelung, die dem Arbeitnehmer die private Nutzung betrieblicher Kommunikationsmittel untersagt, ist jedoch bei weitem kein Allheilmittel, im Gegenteil: die Privatsphäre des Beschäftigten gilt auch am Arbeitsplatz, und sie gilt auch bei der dienstlichen Nutzung. Zwar darf der Arbeitgeber die Einhaltung arbeitsrechtlicher Vorgaben kontrollieren, doch unterliegen diese dem Verhältnismäßigkeitsgrundsatz, und deshalb muss der Arbeitgeber stets eine Abwägung mit dem Persönlichkeitsrecht des Beschäftigten vornehmen – er kommt also nicht umhin, sich mit datenschutzrechtlichen Forderungen auseinanderzusetzen und für deren Umsetzung am Arbeitsplatz zu sorgen.

Arbeitgeber, die ihren Mitarbeitern die private Internetnutzung ausdrücklich erlauben, werden dagegen vor ganz andere Probleme gestellt: als Anbieter von Telekommunikationsdienstleistungen haben sie das Telekommunikationsgesetz einzuhalten und unterliegen damit strengen datenschutzrechtlichen Vorgaben. Weil sich der Arbeitgeber in Unkenntnis der Nutzungsart im Zweifel an das Fernmeldegeheimnis halten muss, ist eine datenschutzgerechte Missbrauchskontrolle nahezu ausgeschlossen. Also die private Nutzung doch verbieten?

Einen Ausweg aus diesem Dilemma bietet die technische Trennung der privaten und beruflichen Nutzung. Durch die Abgrenzung der beiden Nutzungsarten fallen schließlich auch die Rechtsfolgen verschieden aus: je nachdem, ob das Internet aus dienstlichem oder privatem Anlass genutzt wird, muss ein anderer

Rechtskontext zugrunde gelegt werden. Dies erlaubt es zum einen, die private Internetnutzung so zu gestalten, dass das gewohnte Sicherheitsniveau nicht unterschritten werden muss, zum anderen aber auch, dass Kontrollen durch den Arbeitgeber nicht personenbezogen erfolgen müssen. Auf diese Weise lässt sich ein Interessenausgleich zwischen dem Direktionsrecht des Arbeitgebers und dem Persönlichkeitsrecht des Beschäftigten erreichen.
Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten von Bund und Ländern arbeitet derzeit an einer Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz.

3. Telemediengesetz

Das neue Telemediengesetz ist zum 01.03.2007 in Kraft getreten. Unsere Informationsgesellschaft, die im Geschäftsleben, im eGovernment und im Privatbereich immer stärker auf das reibungslose Funktionieren der Informationsverarbeitung und der Internettechnologien baut, benötigt auch eine Rechtsordnung, die dem Recht auf die Privatsphäre und die informationelle Selbstbestimmung gerecht wird. Im Berichtszeitraum hatten die Datenschutzbeauftragten von Bund und Ländern gemeinsam die Gesetzesentwürfe des Elektronischen-Geschäftsverkehr-Vereinheitlichungsgesetzes (ElGVG) intensiv verfolgt und durch Stellungnahmen datenschutzrechtliche Bewertungen vorgenommen. Wir waren insbesondere über den Arbeitskreis Medien an diesem Prozess beteiligt.
Die Datenschutzvorschriften, die zuvor im Teledienstedatenschutzgesetz (TDDSG) bzw. im Mediendienstestaatsvertrag (MDStV) der Länder festgelegt waren, sind durch das Telemediengesetz vereinheitlicht worden. Völlig ungelöst blieb bei der Novellierung allerdings die Frage, wie die notwendige Klarheit durch die Rechtsnorm hergestellt werden soll. Die Abgrenzung der Datenschutzregelungen zwischen dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz ist nicht in der nötigen Deutlichkeit gelungen. Auf positive Legaldefinitionen innerhalb des TMG wurde leider verzichtet. Das Gesetz begnügt sich mit negativ abgegrenzten Definitionen. Damit dürften Streitfälle recht schnell bei den Gerichten zur Entscheidung anstehen.
Als materielle Rechtsänderungen sind zu erwähnen:

- eine neue Vorschrift, die das Verschleiern des kommerziellen Charakters einer Nachricht oder des Absenders verbietet und den Verstoß mit Bußgeld bedroht
- Bestands- und Nutzungsdaten sollen künftig zusätzlich grundsätzlich auch für Zwecke der Gefahrenabwehr zur Verfügung stehen. Auf Betreiben des Bundesrates und mit Zustimmung der Bundesregierung solle damit auch die vorbeugende Bekämpfung von Straftaten ermöglicht werden.

Korrespondierend zum TMG ist im Sommer 2006 der 9. Rundfunkänderungsstaatsvertrag von den Ländern verhandelt und von den Ministerpräsidenten unterzeichnet worden. Zeitgleich mit dem TMG ist er am 01.03.2007 in Kraft getreten. Die bisherigen Datenschutzvorschriften, die in §§ 47ff für Rundfunkanstalten geregelt waren, sind zugunsten eines Verweises auf die Datenschutzvorschriften des TMG gestrichen worden, um auch hier eine Vereinheitlichung bei Rundfunk und Telemedien zu erzielen.

Gruppenprüfung 18

Prüfung, Beratung und Erfahrungsaustausch

Aufwand …

Prüfungen bei öffentlichen Stellen in Niedersachsen sind ausdrücklich Aufgabe des Landesbeauftragten für den Datenschutz. Sie sollen sicherstellen, dass bei den öffentlichen Stellen in Niedersachsen nach den Bestimmungen des Nds. Datenschutzgesetzes verfahren wird. Solche Prüfungen sind stets mit erheblichem Aufwand sowohl für den Prüfer als auch für die geprüften Stellen verbunden. Das Ergebnis bezieht sich naturgemäß auf den überprüften Einzelfall und ist ansonsten kaum übertragbar. In Zeiten, in denen Personal und Sachmittel ständig knapper werden, muss die Frage gestellt werden, ob die vorsorgende Einzelprüfung auf Dauer noch Bestand haben kann.

… und Nutzen

Als Antwort wurde in meinem Hause unter Beteiligung der kommunalen Spitzenverbände das Instrument der Gruppenprüfung entwickelt. Ziel war es, neben den Prüfungsaspekten vermehrt auf Beratung zu setzen und die Ergebnisse in einem Erfahrungsaustausch mit allen Beteiligten so aufzubereiten, dass sie für einen breiten Anwenderkreis übertragbar werden. Voraussetzung für die erfolgreiche Durchführung einer Gruppenprüfung ist die vorherige Festlegung eines Schwerpunktthemas. Hier bieten sich naturgemäß Fragestellungen an, die sich in vielen Bereichen der öffentlichen Verwaltung stellen, so dass die Ergebnisse der Gruppenprüfung Hilfestellung für viele Organisationen geben können und sich das Verhältnis von Aufwand und Nutzen deutlich verbessert.

Aktuelle Fragestellung: Protokollierung in IT-Systemen

Seit Herbst letzten Jahres arbeiten wir an einer Gruppenprüfung zum Themenschwerpunkt „Protokollierung“. Dieses Thema hatte sich aus verschiedenen Nachfragen und Einzelberatungen zu Fragen aus diesem Bereich ergeben. Teilnehmer der aktuellen Gruppenprüfung sind 4 Landkreise und 15 Gemeinden im Raum Diepholz.

Die Durchführung der Prüfung geschieht in zwei Abschnitten; im ersten Abschnitt wird das allgemeine Umfeld und das Schwerpunktthema durch Fragebögen erschlossen. Nach Auswertung dieser Vorab-Informationen findet ein Prüfungsgespräch vor Ort statt, das auch für die Diskussion begleitender Fragestellungen genutzt wird.

Nach Abschluss der Besuche bei den Landkreisen zeichnet sich ab, dass auf dieser Ebene in vielen Bereichen des technisch-organisatorischen Datenschutzes deutliche Fortschritte erkennbar sind. Gleichzeitig wird aber auch deutlich, dass für die datenschutzgerechte Gestaltung von Protokollierungen von IT-Verfahren und IT-Systemen im Alltag oft zu wenig Raum bleibt. Eine der Ursachen hierfür dürfte die auch im kommunalen Bereich grassierende Stellenknappheit nicht nur in den technischen Bereichen sein. Alles in allem hat sich unsere ursprüngliche

Vermutung bestätigt, dass es im Bereich der Protokollierung unter Datenschutzgesichtspunkten Defizite gibt.

Die nächsten Schritte …

Nach Auswertung der schriftlichen Unterlagen sind wir im Frühjahr 2007 wieder intensiv in die Praxis eingetaucht; diesmal bei den Gemeinden. Die Ergebnisse dieser Gespräche vor Ort werden uns für die Größenklassen der Gemeinden die erforderlichen Erkenntnisse liefern, die zu einer abschließenden Beurteilung der Gesamtsituation unverzichtbar sind. Im Anschluss wird mit allen Beteiligten an einer tragfähigen Lösung der gemeinsamen Probleme gearbeitet. Zielsetzung dieser Gruppenprüfung bleibt, konkrete Lösungsansätze für den datenschutzgerechten Umgang mit Protokolldaten zu entwickeln, die möglichst praxisgerecht sind und von allen Verwaltungen in Niedersachsen unmittelbar umgesetzt werden können.

Nach Abschluss der Arbeiten voraussichtlich im Herbst 2007 werden die Ergebnisse unter dem nebenstehenden Link veröffentlicht.

www.lfd.niedersachsen.de
> Service-Angebote > Checklisten
> Protokollierung

Gesprächskreis mit Leitern der Rechenzentren

Von Rechenzentren erwartet man heute nicht nur einen leistungsfähigen und hochprofessionellen Betrieb, sondern auch sichere und datenschutzgerechte Technik und Prozesse. Hier sind Experten gefragt, die die jeweiligen Spezialgebiete abdecken.

Art, Umfang und Ausgestaltung von technischen und organisatorischen Maßnahmen im Interesse des Datenschutzes bei Verfahren der Informations- und Kommunikationstechnik (IT-Verfahren) sind einerseits immer individuell auf den jeweiligen Anwendungsbereich festzulegen und umzusetzen. Andererseits lassen sich sach- und fachgerechte sowie gleichzeitig datenschutzgerechte, angemessene Lösungen nur vergleichbar machen und überprüfen, wenn diese weitestgehend standardisiert werden. Außerdem müssen erfolgreiche Modelle bekannt gemacht und übernommen werden, die sich nach dem „best practices“ Prinzip, also nach den aus der praktischen Erfahrung heraus als bewährt geltenden Modellen herausgebildet haben.

Nach meiner Auffassung würde es insofern nicht ausreichen, wenn wir nur datenschutzrechtliche Beratungen, Kontrollen oder Stellungnahmen in zahlreichen Einzelfällen abgeben und deren Umsetzung im Übrigen häufig dem Zufall überlassen würden. Vielmehr kommt es darauf an, thematisch aufbereitet durch präventive Maßnahmen den Verantwortlichen an zentralen Stellen die Möglichkeit zu geben, sich rechtzeitig planerisch mit den datenschutzrechtlichen Notwendigkeiten auseinanderzusetzen.

Planung, Initiierung und Start

Aus dieser Überlegung heraus haben wir einen Gesprächskreis mit den Leitern, sonstigen Führungskräften und Datenschutzbeauftragten von IT-Betrieben und Rechenzentren initiiert. Die Veranstaltungsreihe ist eingebettet in die Angebote meines Datenschutzinstitutes. Es wurden die Leiter der Rechenzentren und der großen Organisationsbereiche eingeladen, die Dienstleistungen für Hochschulen, Fachhochschulen, Kommunen und die Landesverwaltung erbringen.

Ziel war es, diesen Gesprächskreis als festen Bestandteil eines Netzwerkes zu etablieren und in Abstimmung mit den Teilnehmenden in einem angemessenen zeitlichen Rhythmus die fachlichen Kontakte zu pflegen, um einen höchstmöglichen Nutzwert aus diesem Netzwerk ziehen zu können.
In einer konstituierenden Veranstaltung (1. Gesprächskreis) ging es zunächst darum, die Themenschwerpunkte neuer Technologien und Innovationen zu definieren, die nach den Prioritäten geordnet auf die Agenda der künftigen Veranstaltungen gesetzt werden sollten. In den folgenden durchgeführten Gesprächskreisen (2. bis 4.) wurden bereits die nachfolgend beschriebenen Themenblöcke behandelt:
Im Überblick:

- Portale, Internet-/Intranet-Kopplung, eGovernment, Webhosting
- Identity Management, Verzeichnisdienste, Meta Directory, LDAP, SOI, PKI, Hochschul- und Studenten-Informationssysteme
- Auftragsdatenverarbeitung, Dienstleister-Kunden-Beziehung, SLA und Datenschutz

Für 2007 sind weitere aktuelle Themenblöcke geplant, im Überblick:

- Logging: Datensicherheit & Datenschutz; Beispiel Firewall
- Schutzstufenkonzept, Vorabkontrolle: Empfehlungen für datenschutzkonforme Ziele und praxisnahe Handhabung

Nachfolgend werden die oben genannten, im Berichtszeitraum bereits behandelten Themen beschrieben.

2. Gesprächskreis: „Portale für Internet und Intranet – Datenschutzgerechte Ansätze bei Planung, Entwicklung und Betrieb von Plattformen als Bestandteil einer eGovernment-Umgebung“

Das Angebot von Webseiten im Intranet und im Internet ist zu einem Muss für jede Organisation geworden. Dabei geht es nicht mehr darum, lediglich Informationen bereitzustellen, sondern längst hat sich diese Plattform zu einer interaktiven Komponente der Geschäftsprozesse entwickelt. Datenbank gestützte Speicherung von Inhalten **(Contents)** ermöglichen eine strukturierte Ablage. Eine so genannte **„Metadatenverwaltung“** mit strukturiert beschreibenden Merkmalen von Inhalten erzwingt das Ordnen, Gliedern und Wiederauffinden indizierter Contents. Abgefragte oder gefilterte Inhalte werden durch individuelle oder personalisierte Abfragen mittels dynamischer Seitenaufbereitung zur Laufzeit, also zum Zeitpunkt der Abfrage, generiert und präsentiert. So genannte Web Content Management Systeme **(CMS)** ermöglichen die Trennung zwischen inhaltspublizierender und technischer Betreuung des Systems, also zwischen Fachautoren, Redakteuren, Chefredakteuren und Administratoren. Damit schwindet auch die faktische Notwendigkeit, mehrere technische Plattformen zur physischen Trennung von Informationen vorzuhalten. Stattdessen lassen sich mit einem CMS virtuell die internen Informationen der Firma oder Organisation von den öffentlich zu präsentierenden Informationen und den ggf. für in einer Vertrauensstellung stehenden Extranet-Partnern trennen.
Wirtschaftlichkeitsgesichtspunkte gebieten die Zusammenlegung der Mechanismen, die Vereinheitlichung und Zusammenführung (so genannte Konsolidierung) der Hard- und Softwarekomponenten, die Standardisierung der Geschäftsabläufe (Workflow-Prozesse) und somit die lose Kopplung oder letztlich

die Konsolidierung der Plattformen mit virtueller Trennung über ein Rechte- und Rollenkonzept.
Welche datenschutzrechtlichen Rahmenbedingungen müssen aber bei dieser Strategie der Bündelung und Zusammenlegung berücksichtigt werden? Benutzerverwaltung, Rechteprofile, Zugriffsschutz, Inhaltsbewertung und Grenzen der Integration müssen dabei neu bewertet werden. Der Schutzbedarf der gespeicherten und zu verarbeitenden Informationen bestimmt die Ausgestaltung der technischen und organisatorischen Maßnahmen. In dem Gesprächskreis wurden Ansätze für ein datenschutzgerechtes eGovernment diskutiert, wie auch diese Technologien „datenschutzfit" zu machen sind und wie man sich dem extrem schnellen Wandel von Web Content Management stellen kann. Dabei konnten Erfahrungen des IT-Managements ausgetauscht, Rahmenbedingungen aus Sicht des Datenschutzes von meiner Seite beigesteuert und teils gemeinsame Überlegungen für strategische Ansätze gefunden werden.

3. Gesprächskreis: „Identitäts-Management-Systeme"

Ein Identitäts-Management-System **(IMS)** gilt als ein organisatorischer und technischer Schritt zur Vereinfachung von Rechten im Zugriffsverwaltungssystem (Accessmanagement) von IT-Systemen und IT-Verfahren. Es geht um das Verwalten und Verarbeiten von Identitätsinformationen von natürlichen oder juristischen Personen. Beim Bestreben, dies wirtschaftlich zu gestalten, entsteht schnell der Bedarf, nur ein einziges zentrales System für alle Verfahren einzusetzen, um den Komfort und damit den Nutzwert bei gleichzeitiger Aufwandsreduzierung zu erhöhen. Dabei spielt in der Regel ein Verzeichnisdienst oder Meta Directory eine zentrale Rolle. Gekoppelt über ein Lightweight Directory Access Protocol (LDAP; Protokoll zur Abfrage und Modifikation von Informationen eines Verzeichnisdienstes) wurde bereits ein Prototyp für Hochschulen durch das Projekt SOI realisiert. Allerdings bestehen eine Reihe von unterschiedlichen Definitionen und Ausprägungen, je nach beabsichtigter Funktion.
Es wurde eine Reihe von Fragen behandelt, vor allem:

- Welche datenschutzrechtlichen Rahmenbedingungen müssen bei dieser Strategie der Konsolidierung von IMS-Prozessen berücksichtigt werden?
- Kollidiert dies mit dem datenschutzrechtlichen Zweckbindungsgebot?
- Wie können Anwendungen, z. B. Hochschul- und Studenten-Informationssysteme oder andere Fachverfahren der Verwaltung, eingebunden werden? Welche Maßnahmen müssen entwickelt werden?
- Worauf ist bei der Analyse von Benutzerverwaltung, Rechteprofilen, Zugriffsschutz, Inhaltsbewertung der Daten und Grenzen der Integration zu achten?
- Gibt es im IMS technische und organisatorische Ansätze für datenschutzgerechte Lösungen?
- Wird das Pseudonym als zweite Identität berücksichtigt? Kann die Person über die Verwendung ihrer Identitäten selbst entscheiden?
- Sind in bisherigen Pilotversuchen auch Datenschutzfragen behandelt und gelöst worden?
- Lassen sich vorhandene Lösungen nachträglich datenschutzgerecht gestalten?

Auch in dieser Runde wurden Erfahrungen des IT-Managements ausgetauscht, konkrete Projekte im Hochschulbereich betrachtet und die ergänzende Sicht des Datenschutzes von meiner Seite beigesteuert.

4. Gesprächskreis: „Datenschutz in Service Level Agreements (SLA): Auftragsdatenverarbeitung, Dienstleister-Kunden-Beziehung und ITIL-Prozesse datenschutzgerecht gestalten"

Wurden in der Vergangenheit IT-Systeme in der Verwaltung sehr häufig dezentral vor Ort oder durch kleinere organisatorische Serviceeinheiten administrativ betreut, so ist in den letzten Jahren ein starker Trend zu beobachten, IT-Service mancherorts erstmals organisatorisch zu vereinheitlichen und zusammenzuführen (Konsolidierung), oder in anderen Fällen wieder zu rezentralisieren.

Ziel ist dabei immer, Serviceprozesse zu standardisieren, Services in ihrer Qualität messbar, transparent und kostengünstiger zu gestalten. Dabei müssen zudem Informationssicherheit und Datenschutz sichergestellt werden.

Die Gestaltung des IT-Services (IT-Service-Management) ist dabei geprägt durch eine Dienstleister-Kunden-Beziehung. Für deren organisatorische Umsetzung sind Prozesse notwendig, die sich durch anerkannte best practices nach dem standardisierten Rahmenwerk „ITIL" (IT Infrastructure Library) gestalten lassen. In Dienstleistungsvereinbarungen und Service Level Agreements **(SLA)** werden Regelungen ausgehandelt, die auch Festlegungen zu technischen und organisatorischen Maßnahmen für die Informationssicherheit und den Datenschutz enthalten müssen.

Oft wird übersehen, dass der Auftraggeber (Kunde) in der Rolle mit der primären Verantwortung für Informationssicherheit und Datenschutz bleibt. Die Beauftragung des Dienstleisters verpflichtet diesen zwar zur Umsetzung vereinbarter Maßnahmen und ggf. Anwendung bestimmter Technologien. Das Management der Sicherungsziele, die Definition des Schutzbedarfes und der Anforderungsanalyse bleibt aber ureigene Aufgabe des Auftraggebers als Eigentümer und Gestalter der Fachaufgabe, für die der IT-Service benötigt wird.

Für sie stellen sich also weiterhin vor allem folgende Fragen:

- Welche Konsequenzen ergeben sich aus dieser modularen Situation?
- Welche Erkenntnisse helfen, um ein reibungsloses Miteinander zwischen Auftraggeber und Auftragnehmer zu erzielen?
- Wie können Informations-Sicherheitsrichtlinien, IT-Sicherheitskonzepte, Datenschutzrichtlinien und Vorabkontrollen in hierarchischer Abstimmung zur Optimierung von IT-Service und –Betrieb beitragen?
- Wie sicher lassen sich datenschutzrechtliche Grundziele wie Zweckbindungsgebot und Datenvermeidung/Datensparsamkeit sowie die Gestaltungsziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität beim Betrieb durch Externe erreichen?
- Welche Auswirkungen haben Virtualisierung und Clusterung zentraler Systeme auf Informationssicherheit und Datenschutz?

Bei diesem Veranstaltungsthema lag die Besonderheit vor, dass die Teilnehmenden sowohl von der Auftraggeber-/Kundenseite als auch von der Dienstleisterseite kamen.

Die IT Infrastructure Library (ITIL) ist eine systematische Sammlung von Publikationen, die eine mögliche Umsetzung eines IT-Service-Managements beschreiben. ITIL gilt international als de-facto Standard. Die Beschreibung orientiert sich am Lebenszyklus des Services: Strategie (Strategy), Entwurf (Design), Betriebsüberleitung (Transition), Betrieb (Operation) und Verbesserung (Continual Improvement) und umfasst die Definition der im Betrieb einer IT-Infrastruktur notwendigen Prozesse, Aufbauorganisation und Werkzeuge.

Ein Service Level Agreement (SLA) ist eine Dienstgütevereinbarung zwischen Kunde (Auftraggeber) und Dienstleister (Auftragnehmer). Sie soll wiederkehrende Dienstleistungen für den Auftraggeber in den Kontrollmöglichkeiten transparenter gestalten, indem zugesicherte Leistungseigenschaften wie etwa Reaktionszeit, Umfang und Schnelligkeit der Bearbeitung genau beschrieben werden und dazu die jeweilige Dienstgüte (Servicelevel, Quality of Service) festgelegt wird.

Informationen zu den Terminen und den Inhalten finden Sie auf unserer Website unter

http://www.lfd.niedersachsen.de/
Aktuelles > Datenschutzinstitut Niedersachsen

Beteiligung bei IT-Verfahren des Landes und der Kommunen

19

Der Landesbeauftragte ist rechtzeitig über Planungen des Landes und der kommunalen Gebietskörperschaften zum Aufbau automatisierter Informationssysteme zu unterrichten. Darunter fallen also auch neue IT-Projekte und wesentliche Änderungen bestehender Projekte. Dieser Regelung des § 22 Abs. 2 NDSG wird zwar nicht immer konsequent und nicht immer rechtzeitig und gründlich nachgekommen, so dass eine Beratung in datenschutzrechtlicher oder technisch organisatorischer Hinsicht nicht immer umfassend geleistet werden kann. Bei Nachfragen unsererseits ist jedoch stets umgehend und umfassend die Offenlegung und Beteiligung nachgeholt worden.

Zu begrüßen ist, dass es seit 2006 regelmäßige Gesprächsrunden gibt, die dieses Problem deutlich reduziert haben. Mit dem IT-Dienstleister der Landesverwaltung Informatikzentrum Niedersachsen (izn) fand und findet ein Jour fix statt, um die aktuellen Vorhaben und technischen Entwicklungen zu erörtern. Dabei waren wechselnde Besetzungen – je nach Themenbereich – erforderlich: sowohl mit dem Geschäftsführer, als auch mit den für IT-Sicherheit zuständigen Personen und dem bDSB sowie teilweise den Abteilungsleitern auf der Seite des izn und mit mir, meinem Vorgänger im Amt und dem für technischen und organisatorischen Datenschutz zuständigen Arbeitsgebiets- bzw. Teamleiter meiner Geschäftsstelle wurden und werden regelmäßig Erfahrungen ausgetauscht, Beratungsleistungen erbracht und Maßnahmen, Strategien und Weiterentwicklungen diskutiert. Diese präventive Verfahrensweise stellt schnelle Informationen und Reaktionen sicher. Im Zuge der Gesprächskreise mit IT-Dienstleistern und Rechenzentren der Universitäten, Fachhochschulen sowie mit kommunalen Datenzentralen, den kommunalen Spitzenverbänden in Niedersachsen und dem izn wurde dieser Austausch vertieft.

Darüber siehe Kapitel 18

1. Mitwirkung im Koordinierungsausschuss IT

Der Koordinierungsausschuss IT (KA-IT) dient der ressortübergreifenden Koordination und Abstimmung für Angelegenheiten der Informationstechnik. Unter anderem berät er über alle Fragen von grundsätzlicher Bedeutung für den IT-Einsatz in der Landesverwaltung und wirkt bei den strategischen Vorgaben mit. Vor allem beim IT-Landeskonzept, beim IT-Gesamtplan und den Grundsätzen der Durchführung des landeszentralen IT-Controlling ist der KA-IT zu beteiligen.[1] Zwangsläufig sind in den dort zu beratenden Vorhaben Fragen berührt, die die informationelle Selbstbestimmung, etwa bei Personaldaten oder Bürgerdaten, betreffen. Damit sind technische und organisatorische Maßnahmen für Datensicherheit und Datenschutz auf abstraktem, aber auch auf ganz konkretem Niveau zu bestimmen.

[1] Abschnitt 6 der 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 07.09.2004 (Nds. MBl. S. 563)

Da ein Vertreter des Landesbeauftragten für den Datenschutz aus dem Bereich technischer und organisatorischer Datenschutz als beratendes Mitglied an den Quartalsberatungen teilnimmt, besteht hier stets die direkte Möglichkeit, im frühzeitigen Dialog etwaige Fragen zu klären und beratend einwirken zu können. Insbesondere bei eGovernment-Vorhaben oder Planungen zur Konsolidierung von Technologien wurden technische und organisatorische Rahmenbedingungen diskutiert und einzelne Fragen einer anschließenden materiellrechtlichen Prüfung unterzogen.

2. „mit.niedersachsen" – mit Datenschutz

Projekt IT-Neuorientierung der Landesverwaltung – aber sicher!

Dass Bürgerinnen und Bürger Ihr Recht auf informationelle Selbstbestimmung auch dann behalten und wahrnehmen können, wenn der Staat seine Informations- und Kommunikationstechnik neu organisiert, sollte ohne Frage sichergestellt sein. Damit der Datenschutz auch tatsächlich dem Recht entsprechend greift, müssen Vertreter der Informationssicherheit und des Datenschutzes bei solchen Projekten auch beteiligt werden.

Die niedersächsische Landesregierung hat sich entschlossen, die IT der Landesverwaltung einer umfassenden Neuorientierung zu unterziehen. Neben der technischen Optimierung u. a. durch Vereinheitlichung und Zusammenführung (so genannte Konsolidierung) der zentralen Komponenten steht vor allem eine Neuordnung der personellen und organisatorischen Ressourcen durch Zentralisierung hin zu einem einzigen IT-Dienstleister, dem izn, auf der Tagesordnung. Diese Entwicklung soll von mir konstruktiv begleitet werden, um sehr frühzeitig aus datenschutzrechtlicher Sicht Ansatzpunkte zum Handeln zu identifizieren und durch präventives Handeln zum ökonomischen und gleichzeitig datenschutzfreundlichen Gelingen des Vorhabens beizutragen. Insbesondere ein Rahmenwerk und die technischen und organisatorischen Standardmaßnahmen des Datenschutzes müssen als Bestandteil in die Planungsvorgaben und Projektarbeit gesichert einfließen.

Projektplanung

Im Rahmen der Verwaltungsmodernisierung soll in der so genannten Phase II die Informationstechnik (IT) der Landesverwaltung einer Reorganisation unter den Gesichtspunkten eines modernen IT-Services zugeführt werden. Neben strategischen Fragen sind dabei methodische, organisatorische und technologische Aspekte zu untersuchen und anzupassen. Bereits ab Mai 2005 wurden von uns die als Kabinettsvorlage zugrunde liegenden Konzepte zur Projektplanung, die auch Beschlusslage des Kabinetts wurden, geprüft. Durch die Definitionen von datenschutzrechtlichen Leitplanken wurden von uns Orientierungsleitlinien in das Projekt gegeben.

Projektstart

Ab Sommer 2005 wurde die erste Projektgruppenstruktur durch das Zentrale Informationsmanagement im Niedersächsischen Ministerium für Inneres und Sport (ZIM) gebildet. In dieser Phase war es uns besonders wichtig, Hinweise zu geben, dass elementare Fragen des technischen und organisatorischen Daten-

schutzes thematisch in der Projektarbeit zu verankern sind. Dies erfolgte nach anfänglichen Gesprächen auf Fachebene durch schriftliche Hinweise an das ZIM im September 2005, die ich anlässlich des Teilprojekts Strategiebildung zum Arbeitspaket IT-Landeskonzept als Eckpunkte aus der Sicht von Datenschutz und Datensicherheit gegeben hatte. Diese Anforderungen und Lösungsvorschläge folgten den gesetzlichen Sicherungs- und Gestaltungszielen im NDSG[2] und den erweiterten Sicherungszielen Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz.

[2] § 7 Abs. 2 NDSG

Bei der Realisierung dieser Sicherungsziele sollten insbesondere die folgenden Teilaspekte Beachtung finden: Rollen- und Berechtigungskonzepte für Anwender und Administratoren sollten dem „need to know"-Prinzip folgen. Das heißt, dass Berechtigungen immer bedingen, dass die Kenntnis der Daten und deren Verarbeitung Bestandteil der jeweiligen Aufgabe ist. Das entspricht auch den Prinzipien der Datenvermeidung und Datensparsamkeit. Ferner sind Maßnahmen zur wirksamen Zugangskontrolle zu treffen und die datenschutzgerechte Protokollierung von Systemen und IT-Anwendungen unter Beachtung einerseits der Revisionsfähigkeit und andererseits des Übermaßverbotes zur Protokollierung sicherzustellen. Die Vollständigkeit der Dokumentation der Programme und Verfahren ist zudem zu gewährleisten. Bei der Bildung neuer Kooperationsformen ist besonders sorgfältig auf technische und organisatorische Datenschutzmaßnahmen, insbesondere präventiv gegen Datenmissbrauch zu achten.

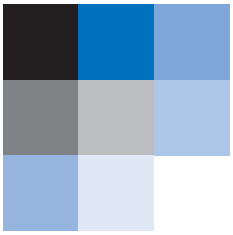
- Neben der Entwicklung einer Sicherheitskonzeption, die begrifflich später als Sicherheitsrichtlinie bezeichnet wurde, gab ich auch Empfehlungen zu einer Reihe von infrastrukturellen Maßnahmen. Insbesondere die beabsichtigte Integration von Telefonie (Voice over IP – VoIP) und Daten aus IT-Verfahren in das vom izn zu betreibende „izn-Net" unter ganzheitlicher Betrachtung von Weit- (WAN) und lokalen Verkehrsnetzen (LAN), erfordert in der Folge bei allen weiteren Konzeptionsschritten ebenfalls eine ganzheitliche Betrachtungsweise. Durch eine vollständige (differenzierungsfreie) Verschlüsselung des Netzes, die unter wirtschaftlichen Aspekten realisiert werden könnte, ließe sich flächendeckend ein durchgängig hohes IT-betriebliches Sicherheitsniveau erreichen, das aus datenschutzrechtlicher Sicht sehr zu begrüßen wäre. Es wurden allgemeine Hinweise zur Anwendung der Schutzstufenkonzeption bei Verschlüsselung und zu Maßnahmen bei Zusammenlegung von Hardware-Ressourcen und Virtualisierung sowie weiteren Einzelfragen gegeben. Schließlich wurde auf die Notwendigkeit hingewiesen, jeweils eine Neubewertung bei erforderlicher quantitativer Aufrüstung der Systeme und Komponenten (sogen. Skalierung) unter technisch-organisatorischer Sicht vorzunehmen.

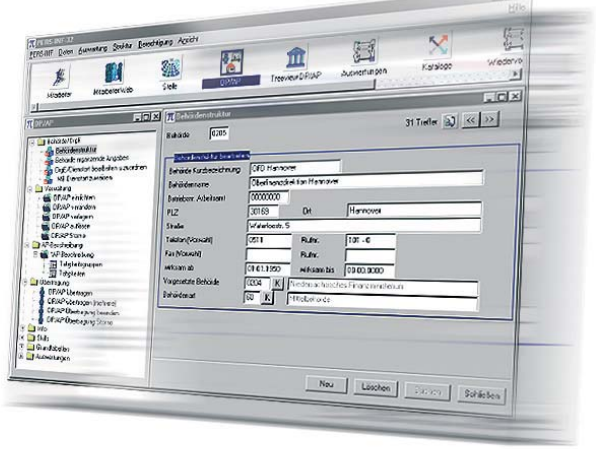
Spezifische Empfehlungen zum izn-net erfolgten ergänzend im Februar 2006 im Hinblick auf die geplante Integration der Daten- und Telekommunikationsnetze mittels Voice-over-IP-Technologien und ergaben so eine datenschutzrechtliche Zwischenbewertung. Insbesondere empfahl ich die Verschlüsselung aller Telefoniedienste und gab zu bedenken, dass ohne ein entsprechendes Basis-Angebot

auf Netzebene entsprechende Überlegungen zu zahlreichen IT-Einzelverfahren und Diensten in jedem Einzelfall erforderlich wären.
Erweiterte Hinweise folgten schriftlich zum IT-Landeskonzept im März 2006. Bereits zum Landeskonzept wurden Fragen zum IT-Sicherheitsprozess aufgeworfen. In den Leitsätzen des CIO wurden ein „ressortübergreifender Sicherheitsprozess“ und ein „landesweites Sicherheitskonzept“ benannt. Gleichzeitig wurde die Ressortverantwortlichkeit für das jeweilige zu realisierende Sicherheitsniveau betont. Unklar blieb, wie das landesweite Sicherheitskonzept entstehen soll, wer es verantwortet und wie es sich von der Ressortverantwortlichkeit abgrenzt oder diese integriert. Schriftliche Antworten dazu sind mir leider nicht zugegangen. Gleichwohl ließ sich die Problematik teilweise im Projektgeschäft aufhellen.
Mit einer Stellungnahme zum izn-Rahmenkonzept, das dem Kabinett im Mai 2006 vorgelegt worden war, wurden weitere Grundpositionen zu den Aspekten integraler Datenschutz, transparentes Schutzniveau, Mindestniveau als Standard, Spielräume für kunden- und anwendungsspezifische Anpassungen (Customizing) und Bezahlbarkeit des jeweiligen Schutzniveaus erläutert.

3. Mitwirkung bei der IT-Sicherheit

Informationssicherheit ist nach allgemein anerkanntem Verständnis der relative Zustand, der durch die Summe aller organisatorischen und technischen Aspekte im Informationsmanagement erreicht wird. Dies schließt die IT-Sicherheit im enger gefassten technischen Sinne ein. Der Begriff Datensicherheit findet sich also inhaltlich in dieser Definition wieder. Da sich die Datensicherheitsmaßnahmen im betrieblichen Sinne zu großen Teilen mit den Datensicherheitsmaßnahmen des technischen und organisatorischen Datenschutzes decken, sollten für die Informationssicherheit die Planungen und Maßnahmen koordiniert werden, die für einen in der Basis einheitlichen Standard wegbereitend sein sollen. Zu diesem Zweck wurde der in meiner Geschäftsstelle zuständige Technikreferent beauftragt, die Projektrolle des Koordinators für IT-Sicherheit in der Projektsäule Technik wahrzunehmen.
Die inhaltlichen Fragen erstreckten sich im Kern auf die Technikbereiche Server- und E-Mail-Server-Konsolidierung, das Betriebsmodell, das Service-Management einschließlich der Gestaltung des IT-Sicherheits-Prozesses, die Technikoptimierung im izn, die Planung der Telekommunikations-Infrastruktur (TK-Infrastruktur) einschließlich der Konvergenz zwischen herkömmlicher Informationsverarbeitung und Datenübertragung sowie künftiger IP-Telefonie im landesweiten Netz und schließlich den landesweit zentralisierten elektronischen Verzeichnisdienst (eDirectory). In zahlreichen Arbeitsgruppensitzungen im Berichtszeitraum und Abstimmungsgesprächen wirkte meine Dienststelle in dieser Rolle an den Arbeitsergebnissen mit.
Durch die fachkundige Detailarbeit des Kompetenzcenters IT-Sicherheit (KITS) des izn und mit externer Unterstützung durch Unternehmensberatungen, die sich auf Informationssicherheitsmanagement (ISM) spezialisiert haben, wurden Konzepte erstellt, die in der Detaillierung der fachlichen Fragen dem aktuellen Kenntnisstand der IT-Sicherheit sowie den Standards und dem Maßnahmenkatalog für Informationssicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen.





Informationssicherheitsmanagement

Soweit die IT-Sicherheit in der Techniksäule thematisiert wurde und durch entsprechende Arbeitspakete und Arbeitsgruppen sowie die o. g. Koordinierungsrolle konkreten Ergebnissen zugeführt worden sind, ist dies als positiv zu bewerten. Auf diese Weise war auch die allgemeine Stärkung und Konkretisierung des technischen und organisatorischen Datenschutzes möglich.

Die Chance, die Querschnittsaufgaben Informationssicherheit und Datenschutz in die Konzeptionsarbeiten in dieser Weise rechtzeitig integrieren zu können, ist jedoch trotz meiner Empfehlung an die Projektleitung und den CIO im April 2006 leider nicht in äquivalenter Weise in den Säulen „Organisation" und „eGovernment" wahrgenommen worden.

Gespräche mit den Datenschutzbeauftragten der Ministerien

Im Rahmen des Amtswechsels habe ich die behördlichen Datenschutzbeauftragten der obersten Landesbehörden zu ausführlichen Erörterungen am 1. November 2006 eingeladen. Da trotz der Migration durch das genannte Projekt mit.Niedersachsen die Verantwortlichkeit für Informationssicherheit und Datenschutz und bestimmte Aufgaben bei den Ressorts und Dienststellen verbleiben, ergaben sich zahlreiche Fragen u. a. bei der Handhabung des Servicemanagements, der Datensicherheits- und Datenschutzmaßnahmen und der damit verbundenen Prozesse. Das für diese Häuser maßgebliche Betriebsmodell beinhaltet – aus datenschutzrechtlicher Sicht – nach unserer Auffassung keine grundsätzlich zu beanstandenden Ausführungen und Regelungen. Im Einzelnen kommt es jedoch auf die Ausgestaltung der einzelnen Dienstleistungsverträge und der Service Level Agreements (SLA) an, wie weit die Schnittstelle zwischen Auftraggeber (Kunde: Ressort, Dienststelle) und Auftragnehmer (Dienstleister: izn) datenschutzrechtliche Besonderheiten aufweist. Die IT-Koordinatoren und Datenschutzbeauftragten der Ressorts sollten daher entsprechend ihrer weiterhin bestehenden Verantwortung für Informationssicherheit (einschließlich IT-Sicherheit) und für Datenschutzfragen auf die angemessene und sachgemäße Umsetzung achten. Dort, wo dagegen die betriebliche Verantwortung des Dienstleisters vorliegt, werden nach dem Konstrukt des Betriebsmodells generische Sicherheitslösungen für Systeme, technische Dienste oder IT-Verfahren mit allgemeinverbindlicher Wirkung vorgegeben. Generisch bedeutet hier, dass für alle gleichermaßen betroffenen Objekte und Kunden dieser Lösung die auf abstrakter Ebene allgemeingültig entwickelten Eigenschaften und Wirkungen gelten. Aber auch hier können einzelne individuelle zusätzliche oder abweichende Maßnahmen für den einzelnen Kunden notwendig werden, die entsprechend im Dienstleistungsvertrag nachzuverhandeln wären.

Ist unsere Privatsphäre der IT schutzlos ausgeliefert?

Was können wir dagegen tun?

Die Informationstechnik im Alltag bietet Komfortgewinn, Vereinfachung und Beschleunigung bei lästigen Routinehandlungen. Technische Innovationen gehen dabei mit immer mehr Datensammlungen einher. Neben den „Segen" gesellen sich also auch schleichende Risiken und Nebenwirkungen für den Datenschutz. Das „Minenfeld Technikinnovation", das das folgende Dossier beschreibt, gilt es, datenschutzrechtlich zu würdigen. Es ist aber dieselbe Technik, die es als Werkzeug dem Datenschutz erst möglich macht, sich mittels geeigneter Maßnahmen für die informationelle Selbstbestimmung durchzusetzen!

Im Verbund stark: Mitarbeit im Arbeitskreis „Technik" als arbeitsteilige Plattform

Viele datenschutzrechtliche Themen – auch gerade im technisch-organisatorischen Bereich – betreffen nicht nur Niedersachsen; sie sind auf breiterer Ebene und Bundesland übergreifend zu behandeln. Überall gelten gleichermaßen die Gestaltungsziele der Informationssicherheit einschließlich der IT-Sicherheit: Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Der Schutz personenbezogener oder personenbeziehbarer Daten erfordert darüber hinaus als Maxime eine datensparsame Verfahrensgestaltung, die Zweckbindung der Daten sowie die Transparenz und die Revisionsfähigkeit der Verfahren.

Die Datenschutzbeauftragten der Länder und des Bundes haben sich unterhalb ihrer Konferenz in Arbeitskreisen organisiert, um allgemeine Entwicklungen und Länder übergreifende Aspekte zu diskutieren und gemeinsame Produkte auf den „Markt" zu bringen. Bei der Bewertung von technischen Entwicklungen gilt es, Entschließungen vorzubereiten und Orientierungshilfen, Beratungsergebnisse und Standards zu formulieren, die eine datenschutzrechtlich unbedenkliche bzw. datenschutzfreundliche Ausgestaltung definieren. Dabei hat sich der Arbeitskreis für technische und organisatorische Datenschutzfragen (AK Technik) als effiziente Plattform erwiesen, um arbeitsteilig die Themen zu behandeln und auf diese Weise zwischen den Datenschutzbeauftragten von Bund und Ländern gegenseitige Unterstützung und Ergänzung zu erzielen.

Technische Entwicklungen beobachten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung im Frühjahr 2006 ihren unter der Federführung des LfD Mecklenburg-Vorpommern stehenden Arbeitskreis Technik beauftragt, künftig regelmäßig zu den Konferenzen einen Kurzbericht über aktuelle und künftige technische Entwicklungen vorzulegen. Damit sollen die Datenschutzbeauftragten frühzeitig Gelegenheit haben, die datenschutzrechtlichen Aspekte neuer Technikentwicklungen zu erörtern und ggf. entsprechend zu reagieren. Zuletzt wurden als Themenbereiche elektronische Ausweisdokumente, Biometrie in Aus-

20

weisen und Verbindung von Videoüberwachung, Biometrie und RFID genannt. Im einzelnen:

Technik im Kombipack: Überwachung perfekt?

Videoüberwachung, biometrische Identifikationsverfahren und Anwendungen mit Funkchips (RFID-Tags) sind bereits heute in einigen Anwendungsfeldern weit verbreitet oder stehen vor ihrer flächendeckenden Einführung. Es ist davon auszugehen, dass diese Technologien funktional und logisch miteinander vernetzt werden und zur Gewinnung von sehr präzisen Bewegungsprofilen von Personen herangezogen werden können. Die Verbindung zwischen biometrischen Verfahren mittels Gesichtserkennung mit Videoüberwachungstechnik stellt beispielsweise einen weiteren Schritt dar zur unbemerkten Identifizierung von bestimmten Personen oder – bedenklicher – anlassunabhängig von beliebigen Personen. Sofern diese Technik mit RFID-Chips kombiniert wird, die den Bezug zu der Person herstellen, kann durch diese Chips die Beobachtung und Aufzeichnung ausgelöst werden und sogar die Personeninformationen von Kamera zu Kamera weitergereicht werden. Damit könnte eine fast unterbrechungsfreie Verfolgung mobilen Verhaltens von Personen ermöglicht werden.

Biometrische Verfahren sind technische Verfahren zur Erkennung eindeutiger körperlicher Merkmale eines Menschen. Das Thema wird weiter unten näher behandelt.

Funkchips – über die niedersächsischen Grenzen hinweg

Im Arbeitskreis „Technische und organisatorische Datenschutzfragen“ wurde im Berichtszeitraum intensiv an der technischen und datenschutzrechtlichen Bewertung der Entwicklungen zu Funkchips (RFID) gearbeitet. Das Thema wird weiter unten separat behandelt.

(siehe Seite 68)

Risiken erhöht durch Internet-Telefonie

Voice over IP (VoIP) ist die Übertragung von Sprachinformationen mittels der Internet-Technologie. Was herkömmlich als analoge Telefonie oder später als digitale Kommunikation (ISDN – Integrated Services Digital Network) über eigene Leitungen funktioniert, soll nun – wie die Internetkommunikation auch – über deren beliebige Draht- oder Funk-Verbindungen mit Hilfe desselben Internetprotokolls erfolgen. Das kann sowohl als Internet-Telefonie weltweit als auch in geschlossenen Netzen als Ersatz eines herkömmlichen Privatnetzes von Unternehmen, Behörden oder sonstigen Organisationen im so genannten Intranet geschehen. Diese Variante des Telefondienstes wird bereits vielfach genutzt, weil sie kostengünstiger und qualitativ durchaus ebenbürtig zur klassischen Telefonie ist, jedoch zusätzliche, kombinierbare Funktionen und flexible Einsatzszenarien zulässt. Noch immer viel zu wenig bewusst ist jedoch, dass die bekannten Sicherheitsprobleme des Internets damit auch beim Telefonieren wirksam werden können. Die Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch

VoIP (Voice over Internet Protokol) Sprachübertragung über Leitungswege, die mit Hilfe eines einheitlichen Protokolls – des Internet Protokolls (IP) – Datenkommunikation jeder Art ermöglicht (Sprache, Text, Musik, Video, Anwendungen, Datenbankverbindungen usw.)

SPIT (Spam over Internet Protocol Telephony) sind unerwünschte, massenweise erzeugte Anrufe von VoIP-Telefonen. Die Anrufe werden automatisiert vorgenommen und können nahezu beliebig wiederholt werden.

VoIP-Telefone sind Telfongeräte, die über eine Internet- oder Intranet-Verbindung oder an Computer angeschlossen werden. Sie nutzen das Übertragungsprotokoll des Internet (IP), bei dem

die Sprachdaten in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt werden.

Blockade eines Dienstes (DoS – Denial of Service) ist ein Angriff auf einen Rechner oder ein Netzwerk mit dem Ziel, einen oder mehrere der dort laufenden IT-Dienste arbeitsunfähig zu machen. Mit einer verteilten Dienstblockade (DDoS – Distributed Denial of Service) lässt sich der Angriff koordiniert von mehreren Rechnern aus steuern.

Als geeignetes **VoIP-Verschlüsselungsverfahren** gegen das Abhören und gegen Manipulationen von IP-Telefonaten bei der Übertragung von Mediendaten der IP-Telefonie und zu deren Kontrolle gilt derzeit z. B. der Einsatz der beiden Protokollerweiterungen „Secure Real-Time Transport Protocol" **(SRTP)** und Real-Time Streaming Protocol **(SRTSP).** Das wird auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI; http://www.bsi.bund.de/gshb) im Maßnahmenkatalog (M 5.135) zum IT-Grundschutz empfohlen, um damit Vertraulichkeit, Authentizität und Schutz gegen so gen. Replay-Angriffe (Wiedereinspielen von Nachrichten) für die Medienübertragung zu erreichen. Vgl. hierzu auch das vom BSI registrierte Schutzprofil (Protection Profile) BSI-PP-0012-2005 „Low Assurance Protection Profile for a Voice over IP Infrastructure, Version 1.1/Zertifizierungsreport PP-0012". Ziel dieses Schutzprofils ist es, funktionale Anforderungen und Vertrauenswürdigkeitsanforderungen für Voice over IP (VoIP) Infrastrukturen zu spezifizieren. Das Schutzprofil definiert die Sicherheitsanforderungen von VoIP-Infrastrukturen für die Identifikation und Authentisierung von Benutzern, das Management der Infrastruktur, die Protokollierung und den Selbstschutz des Systems. Quelle: http://www.bsi.bund.de/cc/pplist/pplist.htm#ip

Entschließung der DSB-Konferenz:
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom Herbst 2005 auf das Problem hingewiesen, dass die Sicherheits- und Datenschutzrisiken der VoIP-Technologie bei den Nutzern kaum bekannt

auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Der ungesicherte Einsatz von VoIP ist grundsätzlich mit deutlich größeren Risiken verbunden, weil die VoIP-Systeme die Sicherheitsrisiken der IP-Welt erben und gleichzeitig die meisten aus der herkömmlichen Telekommunikationswelt behalten. In vielen Einzelanfragen und anlässlich der Verwaltungsmodernisierung der Landesverwaltung (siehe „Projekt mit.Niedersachsen") haben wir uns mit den technischen Maßnahmen auseinandergesetzt.

Alte und neue offene Scheunentore

Zu den o. g. Sicherheitsproblemen gehört auch, dass das Phänomen unerwünschter massenhafter Kontaktversuche – ähnlich dem bei elektronischen Mails leidlich bekannten und allseits erlittenen SPAM-Mails – zunehmend auch für die Internet-Telefonie relevant wird: Das Kunstwort „SPIT" steht für das massenweise Anrufen von VoIP-Telefonen (siehe Erklärung im Kasten). Die Auswirkungen sind „Klingelrundrufe", die Überflutung mit Sprachpaketen bis hin zur technischen Blockade. Die bereits bekannten automatisierten Werbeanrufe können somit im Internet wesentlich kostengünstiger und effizienter vollzogen werden, weil vielfältige Standardtechnik des Internet genutzt wird und die Verbindungskosten vergleichsweise gering sind. Da unerwünschte Telefonate noch lästiger sind und wegen der sofortigen Aufmerksamkeit und Reaktion noch massiver in die Privatsphäre eingreifen als E-Mails, stehen neue Herausforderungen für die im IT-Bereich tätigen Sicherheitsexperten bevor, um wirksame technische Maßnahmen (z. B. SPIT-Filter) zu entwickeln.
Ein weiteres Sicherheitsproblem ist, dass die Inhalte und die näheren Umstände der VoIP-Kommunikation wegen der meist fehlenden Verschlüsselung ausgespäht werden können. Wenn so die Authentifizierungsdaten erlangt würden, könnten Angreifer kostenlose Anrufe führen, Schadsoftware einschleusen, Daten ausspähen oder manipulieren sowie Systeme sabotieren. Nicht zuletzt könnte das Sicherheitsniveau der vorhandenen Datennetze insgesamt beeinträchtigt sein, sofern sie für den VoIP-Sprachdatenverkehr mitgenutzt werden.
Aufgrund der Marktöffnung weltweit wären zusätzlich auch Anbieter von VoIP-Diensten mit Sitz im außereuropäischen Ausland Dienstleister, wo ein geringeres Niveau der Datenschutzanforderungen gilt als in der EU. Die VoIP-Kunden und Nutzer könnten unmittelbar mit ihren personenbezogenen Daten betroffen und gefährdet sein.

Hersteller, Anbieter und Anwender von VoIP-Produkten und –Lösungen bleiben daher aufgefordert,

- durch angemessene technische und organisatorische Maßnahmen für eine sichere und datenschutzgerechte Nutzung von VoIP zu sorgen,
- geeignete Verschlüsselungsverfahren (siehe Kasten zu „SRTP") für VoIP anzubieten und angebotene zu nutzen,
- VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und
- bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen bei ganzheitlicher Betrachtung und unter Berücksichtigung des Schutzbedarfes den Risiken angemessene Sicherheitsmaßnahmen entwickelt und umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

Diese Grundsätze aus der datenschutzrechtlichen Sicht zur IP-Telefonie sind im Berichtszeitraum in einem Großprojekt der Landesverwaltung konkret von mir thematisiert worden. Im Projekt „mit.Niedersachsen" der Niedersächsischen Landesregierung mit dem Ziel, die IT der Landesverwaltung einer umfassenden Neuorientierung zu unterziehen, stand auch die Zusammenführung der Daten- und der Sprachkommunikation zu einem einheitlichen (konvergenten) Netz für geschätzte 80.000 Anschlüsse auf der Agenda. Bei der Gestaltung der technischen Anforderungen waren wir mit der Formulierung von technischen und organisatorischen Anforderungen des Datenschutzes etwa 18 Monate beteiligt. Insbesondere die Frage der genannten Verschlüsselung wurde in einer Arbeitsgruppe intensiv beraten, ebenso wie der Schutzbedarf und zahlreiche Aspekte innerhalb des vorläufigen IT-Sicherheitskonzeptes für die Infrastruktur des geplanten Telekommunikationsnetzes. Dabei hat sich die Zusammenarbeit mit den für die Fragen der IT-Sicherheit Verantwortlichen als sehr konstruktiv erwiesen – ein Beispiel mehr dafür, dass bei sehr großen Projekten Datenschutz und Datensicherheit rechtzeitig und eng zusammenarbeiten müssen und können, um verspätete Nachbesserungen, die überproportional Aufwand und Kosten verursachen würden, zu vermeiden.

Fortschritt kann auch Rückschritt sein: Mit Quantenphysik Vertraulichkeit gefährdet?

Im Markt noch nicht ausgereift präsent, aber auch keine reine Fiktion mehr ist der Blick in die Zukunft von Wissenschaftlern, die Effekte der Quantenphysik für so genannte Quantencomputer nutzbar zu machen. Insbesondere Hochleistungsrechner, die im Bereich der Verschlüsselung Spezialaufgaben zu bewältigen haben, könnten einen signifikanten Entwicklungssprung erfahren. Zu diesen Aufgaben gehört das Brechen heute üblicher Verschlüsselungsverfahren (Kryptographie; Näheres siehe nebenstehender Kasten). Da hier noch geforscht wird und bisher nur unter Laborbedingungen befriedigende Ergebnisse vorliegen, steht das Problem derzeit zwar noch nicht an. Allerdings ist die Quantenkryptographie auch die Basis dafür, die anstehenden Probleme zu lösen, denn Seiteneffekte könnten auch dazu genutzt werden, neue Formen geheimer Kommunikation zu entwickeln. Dabei wäre jeder Abhörversuch durch die Angegriffenen bemerkbar und die Kommunikation kann abgebrochen werden, bevor der Angreifer Erfolg hatte.
Im November 2006 zeigte sich, dass sich Vor- und Nachteile ein Kopf-an-Kopf-Rennen liefern. Es gelang US-Wissenschaftlern des Massachusetts Institute of Technology (MIT) in einer quantenkryptographisch verschlüsselten Nachricht bis zu 40 % der Übertragung unbemerkt abzuhören, wenngleich dieser Versuch in einer Simulation und unter Laborbedingungen erfolgte.

sind. Sie forderte die Hersteller, Anbieter und Anwender auf, das Fernmeldegeheimnis zu wahren. In der VoIP-Praxis fehlt es im Gegensatz zur herkömmlichen Technik oft an Sicherheitskonzepten.

Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28.10.2005 in der Hansestadt Lübeck http://www.sachsen-anhalt.de/LPSA/index.php?id=20270

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte ursprünglich eine umfassende Orientierungshilfe zu VoIP geplant. Im Oktober 2005 gab das BSI eine Sicherheitsstudie zu VoIP heraus. Im Jahre 2006 zeichnete sich ab, dass das BSI in der Folge eine Technische Richtlinie zu VoIP plant. Der AK Technik hat daher beschlossen, Beiträge aus Sicht des materiellrechtlichen, technischen und organisatorischen Datenschutzes für diese Richtlinie zu erarbeiten und insofern die Zusammenarbeit mit dem BSI zu fördern.

„VoIPSEC Studie zur Sicherheit von Voice over Internet Protocol", Oktober 2005, Bundesamt für Sicherheit in der Informationstechnik (BSI), www.bsi.bund.de

Verschlüsselungsverfahren (Kryptographie) bisheriger Art ermöglichen einen sicheren Schlüsselaustausch über öffentliche Datenleitungen. Die Sicherheit ist zwar sehr hoch, allerdings letztlich trügerisch, denn sie ist nur relativ. Das liegt daran, dass zwar zwei große Primzahlen miteinander sehr schnell multipliziert werden können, aber der rückwärtige Weg schwierig ist. Denn es ist nur sehr rechenaufwändig und zeitraubend möglich, das Produkt wieder in seine zugrunde liegenden Faktoren zu zerlegen, wenn diese unbekannt sind. Der Angreifer, der also einen Schlüssel knacken will, muss sehr hohen Aufwand treiben, um die als Schlüssel dienenden Primzahlen zu rekonstruieren. Die Sicherheit des Schlüssels ist demnach abhängig von der Rechenleistung, die ein potenzieller Lauscher in den Angriff investiert. Die Sicherheit ist also relativ zum Aufwand.

Mit Quantenphysik wird ein Teilbereich der Physik bezeichnet, der sich mit dem Verhalten und der Wechselwirkung kleinster Teilchen befasst.
Die **Quanteninformatik** ist die Wissenschaft von der Informationsverarbeitung mit Informationsträgern, die quantenmechanische Phänomene ausnutzen und sich so in wesentlichen Eigenschaften von klassischen Informationsträgern unterscheiden. Berechnungen sind wesentlich schneller durchführbar als mit herkömmlicher Computertechnik.

Nanotechnologie und Mikroelektronik
Unter Nanoelektronik versteht man integrierte Schaltkreise mit Strukturbreiten von weniger als 100 Nanometer. Schon heute liegt in der Mikroelektronik die Größenordnung von Transistoren eines handelsüblichen Mikroprozessors im Bereich der Nanotechnologie. Sie sind 0,065 Mikrometer (also 65 Nanometer = 65 Milliardstel Meter) groß. Schaltkreise können aber auch durch so genannte Lithographie gefertigt werden, die eine Strukturbreite von nur 45 Nanometer erreichen. Für das nächste Jahrzehnt wird mit einer weiteren Miniaturisierung bis auf 23 Nanometer gerechnet. Aufgrund der physikalischen Grenzen ist dann ein radikaler Technologiewechsel erforderlich.

Fraglich ist derzeit, wie lange es dauern wird, bis es verbesserte Verfahren gibt, die die herkömmliche und eines Tages geknackte Verschlüsselungstechnik adäquat ersetzen können. In einer Welt, in der die Vertraulichkeit schützenswerter Information und Kommunikation nur durch wirksame Verschlüsselung sichergestellt werden kann, kann sich die Gesellschaft und jedes Individuum einen solchen Schwebezustand nicht leisten. Wir werden diese Forschungsvorhaben deshalb mit besonderem Interesse verfolgen.

Revolution „unter der Grasnarbe“ in Sicht: Nanotechnologie für die Informationstechnik

In den Anwendungsbereichen der Nanotechnologie ist ebenfalls Aufmerksamkeit geboten. Hier geht es um die Trennung, den Zusammenbau und die Verformung von Werkstoffen in der Größenordnung von Atomen und Molekülen. Ein Nanometer hat die Größe eines Milliardstel Meters.
Es handelt sich um eine der maßgeblichsten technologischen Revolutionen der Zukunft. Sie wird völlig neue Basislösungen für die Wissenschaft, die Technik und die Gesellschaft insgesamt hervorbringen. Erheblicher Förderaufwand wird bereits aufgebracht. Vor allem neue Werkstoffe, chemische und physikalische Eigenschaften mit unüberschaubaren biologischen und ökologischen Auswirkungen lassen selbst die Wirtschaftskonzerne in Studien die Forderung aufstellen, zunächst mit Bedacht die Technologiefolgen zu erforschen, statt sogleich die Anwendungen zu realisieren.
Absehbares Ziel der Nanotechnologie ist die weitere Miniaturisierung der Halbleiterelektronik und der Optoelektronik. Damit wird das Ziel erreichbar, Funktionen auf derart kleinen Flächen unterzubringen, dass die Erkennbarkeit in Alltagsgegenständen nicht mehr gegeben ist. Bereits heute ist ein Funkchip mit der Baugröße von 1 Millimeter gebaut worden. Im Nanobereich wäre die Dimension der Miniaturisierung noch erheblich extremer.
Die Nanotechnologie birgt nach meiner Ansicht in der technischen Entwicklung erhebliche Risiken für die informationelle Selbstbestimmung, weil unbemerkt Technik zur Anwendung kommen kann, ohne dass sich der Mensch dem entziehen kann.
Es bleibt zu beobachten, inwieweit es auch Innovationen oder Versäumnisse für die Sicherung der informationellen Selbstbestimmung geben wird. Es ist daher die Grundforderung zu erheben, bereits im Forschungsstadium rechtzeitig Lösungen im Interesse der informationellen Selbstbestimmung zu berücksichtigen, das heißt, den Datenschutz gewissermaßen bereits in die Entwicklungen einzubauen.
Im Folgenden werden Themenbereiche des technischen und organisatorischen Datenschutzes dargestellt, die im Berichtszeitraum einerseits durch den Arbeitskreis Technik gemeinsam bearbeitet worden sind und andererseits auch in konkreten Fragestellungen aus der niedersächsischen Landessicht zu bearbeiten waren.

Getrennter Ansatz, gemeinsame Wege: Informationssicherheit und Datenschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit den in 2005 verabschiedeten Versionen 1.0 der BSI-Standards für Informationssicherheit sowie den in 2006 überarbeiteten Grundschutzkatalogen einen wichtigen Schritt in Richtung Standardisierung und Zertifizierung von Maßnahmen zum Schutz der Informationssicherheit einschließlich der informationstechnischen Sicherheit (IT-Sicherheit) unternommen.

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dieses in Deutschland weithin bekannte, anerkannte und kostenlos verfügbare Regelwerk als ausgezeichnetes Medium erkannt, um datenschutzrechtliche Inhalte mit den Anforderungen an Informationssicherheit abzustimmen und an geeigneter Stelle einzubringen. Eine entsprechende Arbeitsgruppe hat erste Ergänzungen vorgelegt und mit dem BSI abgestimmt. Mit der Veröffentlichung in den offiziellen Standards und Katalogen wird spätestens in 2008 gerechnet.

Wie sich in großen Organisationen die Themen Informationssicherheit und Datenschutz sinnvoll kombinieren lassen und bisher getrennte Prozesse, miteinander verzahnt, zu schnelleren Ergebnissen führen können, ist im Berichtszeitraum am Beispiel des Projektes mit.Niedersachsen zu erkennen, an dem wir uns konstruktiv beteiligt haben.

Die BSI-Standards für Informationssicherheit umfassen derzeit die Teile:

- 100-1: Managementsysteme für Informationssicherheit
- 100-2: IT-Grundschutz Vorgehensweise
- 100-3: Risikoanalyse auf Basis von IT-Grundschutz

Die Grundschutzkataloge umfassen für unterschiedlich zu klassifizierende IT-Verbünde jeweils die passenden empfohlenen Maßnahmen

www.bsi.de/gshb/index.htm

siehe dort Kapitel 19

Datenschutzmanagement: richtiger Anspruch – in der Praxis noch selten umgesetzt

Die tragenden, strukturellen Prinzipien des Datenschutzrechts (Datensparsamkeit, Datenvermeidung, Zweckbindung, Verhältnismäßigkeit) sind materiellrechtliche Gebote des Datenschutzes mit Verfassungsrang. Sie umzusetzen bedeutet in den meisten Fällen, technische und organisatorische Maßnahmen ergreifen zu müssen, die die Informationsverarbeitung erst in die Lage versetzen, rechtmäßig ausgestaltet zu werden.

Ich bin davon überzeugt: Erst mit dem Erreichen einer solchen sicheren Grundlage können Unternehmen und Behörden einen funktionalen Erfolg bei den IT-Verfahren für die Geschäftsprozesse bzw. Verwaltungs- und eGovernment-Prozesse ermöglichen. In der Praxis tun sich Management, Behördenleitungen oder Entscheider sowie Fachverantwortliche und IT-Verantwortliche nach unseren Beobachtungen im Berichtszeitraum häufig noch immer schwer, die notwendigen Rahmenbedingungen zu schaffen, um diese Ziele strukturell und systematisch in Ihrer Organisation umzusetzen. Das hat offenbar zum Teil Kosten- bzw. fiskalische Gründe, zum Teil hat es seine Ursache aber auch darin, dass das Managen von Informationssicherheit, Datenschutz und IT zu oft noch nicht den Weg in die Vorstände und Behördenleitungen gefunden, den Rang einer „Chefsache" also noch nicht erlangt hat. Der Lernprozess ist aber in sehr vielen Bereichen – zunächst bei großen Organisationen – erkennbar zum Laufen gekommen.

Es führt auch nur ein Weg – derzeit erkennbar – zum Ziel: Ein wirksames **präventives und auf Dauer angelegtes, strukturelles Datenschutzmanagement** ist zwingend geboten, um rechtzeitig vor der Einführung neuer Tech-

nologien und IT-Verfahren bereits in der Planungsphase zu den erforderlichen Erkenntnissen und Maßnahmen zu kommen. Der Lebenszyklus eines Datenschutzmanagements ist mit der Planung aber nicht beendet. Es umfasst auch weitere Phasen in der Entwicklung und im Betrieb und erfordert, dass festgelegter Korrekturbedarf in den Entwicklungsprozess zurückgegeben wird. Es entsteht also insgesamt ein sinnvoller rekursiver, prozesshafter Kreislauf des Datenschutzmanagements, wenn alle Beteiligten mit ihrer Rolle und Verantwortung eingebunden worden sind.

Datenschutzmanagement steht nicht isoliert

Um zu ökonomisch vertretbaren Aufwänden zu kommen, bietet es sich an, die Prozesse des ebenfalls erforderlichen Informationssicherheitmanagements (einschließlich der IT-Sicherheit) mit denen eines Datenschutzmanagements zu synchronisieren. Das bedeutet z. B., dass die Erstellung eines IT-Sicherheitskonzepts mit einer Vorabkontrolle und/oder der Erarbeitung eines Datenschutzkonzepts zeitlich verzahnt erfolgen sollte. Damit werden unnötige Doppelarbeiten oder gar widersprüchliche Maßnahmen vermieden und die Chance steigt, dass die Akzeptanz bei den Handlungsverantwortlichen wächst.

In zahlreichen Anfragen durch privatwirtschaftliche Unternehmen sowie öffentlich-rechtliche und privatrechtliche Organisationen konnten wir beratend dieses organisatorische Modell vorstellen und empfehlen und die erforderlichen Maßnahmen in unterschiedlicher Tiefe und Intensität aufzeigen.

Funknetze – die rasante Entwicklung geht weiter

In meinem letzten Tätigkeitsbericht hatte ich mich ausführlich mit den Besonderheiten von Funknetzen wie Bluetooth und Wireless LAN (WLAN) befasst; zwischenzeitlich liegt für diesen Bereich eine umfassende Orientierungshilfe des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vor. Sie ist unter dem Titel „Datenschutz in drahtlosen Netzen“ erschienen und kann von meiner Web-Seite heruntergeladen werden. (www.lfd.niedersachsen.de > Service-Angebote > Technische Hilfen > Drahtlose Netze)

Darüber hinaus wird seitens der Industrie bereits an neuen drahtlosen Netzen gearbeitet, die schon bald die USB-Verkabelung von Geräten im Kurzstreckenbereich ersetzen und einen breitbandigen Datenaustausch zwischen den angeschlossenen Geräten ermöglichen soll. Welche neuen Gefahren eine derartige Technik mit sich bringt, ist heute noch nicht abschließend bewertbar – wir werden aber die Entwicklung verfolgen.

IEEE 802.11n ist der derzeit in der Entwicklung befindliche Standard für **breitbandiges Wireless Local Networking (WLAN)**. Er wird voraussichtlich Mitte 2007 verabschiedet. Es werden Datentransferraten von brutto 540 (bis 600 MBit/s) erreicht und das lizenzfreie Frequenzband von 2,400 bis 2,485 GHz, optional auch 5 GHz als zusätzliches Band genutzt.

USB = Universal Serial Bus; Steckverbindungs- und sogen. Datenbussystem für PC und Notebooks

Biometrische Verfahren – weiterhin nicht ohne Vorbehalte

Die Biometrie ist die Wissenschaft der Körpermessung am Lebewesen. Die Nutzung biometrischer Verfahren zur **Personenidentifikation** (Erkennen bestimmter Personen) und **Personenverifikation** (Erkennen der Übereinstimmung vorgegebener Merkmale mit den Merkmalen, die eine anwesende Person präsentiert) ist bereits seit ein paar Jahren im IT-Markt präsent. Bekannteste Anwendungsfälle hierfür sind die Zugangssicherungen von Hochsicherheitsbereichen

in Kraftwerken, Banken oder militärischen Sektoren (Verifikation) oder die automatisierte Erkennung gesuchter Personen (Identifikation). Bei beiden Varianten müssen vor der erstmaligen Nutzung des Verfahrens ausgewählte Merkmale der betroffenen Person vermessen und mathematisch komprimiert gespeichert worden sein. Bei Kontrollen werden dann die aktuellen Messwerte mit den komprimierten Werten verglichen.

Auch wenn sich noch kein vollständig flächendeckender Einsatz durchgesetzt hat, bietet die Industrie doch bereits eine Reihe technologischer Lösungen an, die die Erkennung unterschiedlicher biometrischer Merkmale des Menschen zum Gegenstand haben. Knapp hundert deutsche Unternehmen stellen aktuell biometrische Produkte her oder befassen sich mit der Systemintegration (BITKOM e. V. 11. Juli 2007 www.bitkom.org/Default_47092.aspx). Insbesondere die Branchen Einzelhandel und Banken weisen für Biometrie-Technologien viele Einsatzmöglichkeiten auf.

Als Vorteil gegenüber herkömmlichen Verfahren wird vor allem angeführt, dass Ausweise oder Passwörter vergessen, gestohlen, gefälscht oder bewusst weitergegeben werden können, während Fingerabdruck, Iris, Gesicht oder Stimme untrennbar mit der Person verbunden sind.

Erkennungsmerkmale

Im Mittelpunkt biometrischer Verfahren stehen bisher vor allem physiologische und verhaltensbasierte Merkmale.

Physiologische biometrische – auch genannt passive – Merkmale sind Körpermerkmale einer Person, die sich nicht oder nur sehr geringfügig über einen längeren Zeitraum verändern. Das sind insbesondere Gesicht, Augen-Iris, Augen-Retina, Finger, Handgeometrie, Venenmuster, Ohr oder DNA.

Verhaltensbasierte biometrische Merkmale dagegen – auch aktive Merkmale genannt – können sich zeitlich verändern und bei jeder neuen Erfassung anders ausfallen. Beispiele sind insbesondere: Unterschrift (dynamisch/statisch), Gestik und Mimik beim Sprechen, Gang, Stimme und Sprechverhalten oder das psychometrische Merkmal Tippverhalten an der Tastatur.

Auch eine Kombination **biometrischer Merkmale oder der Methoden,** ist möglich, zum Beispiel die Erfassung des Gesichts und der Gesichtsdynamik beim Sprechen, kombiniert mit einer Stimmerkennung. Sofern eine eindeutige Identifikation angestrebt wird, ist jedoch das Problem zu lösen, das bei unterschiedlichen Ergebnissen der Messungen entsteht. Kombinationen können zur Erhöhung der Erkennungsrate und Senkung der Fehlerrate führen.

Überwiegend unbekannt aber sind noch weitergehende Methoden. Es gibt bereits Forschungsansätze, Entwicklungen und Projekte, die noch weitere biometrische Erkennungsmethoden zum Einsatz bringen wollen. Jeder Mensch ist in vielen Hinsichten ein Unikat. So hatten wir beispielsweise Gelegenheit, im Sommer 2005 Kenntnis über neue Forschungsansätze zu erlangen:

Die Identifikation des Menschen anhand von **Herzsignalen** als eindeutige Signatur mittels elektrischer, magnetischer, akustischer, optischer, chemischer und thermischer Messung sei möglich, erklärte bei einem von uns besuchten Symposium des CAST e. V. der Gründer der Thinsia GmbH.

Ein **Algorithmus** in der Informatik ist eine genau definierte Handlungsvorschrift zur Lösung eines Problems oder einer bestimmten Art von Problemen in endlich vielen Schritten. Man bezeichnet also die Art der programmtechnischen Lösung der biometrischen Verarbeitung als **biometrischen Algorithmus**.

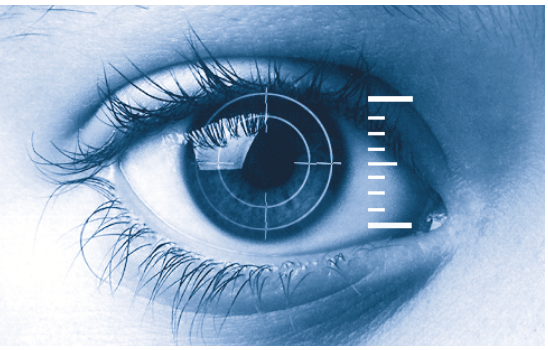
Biometrische Erfassung und Verarbeitung kann mit **Merkmalskombinationen** angewendet werden. Man unterscheidet

- multimodal, also unter Anwendung zweier oder mehrerer Modalitäten (z. B. Finger- und Gesichtsmessung)
- multialgorithmische Messung also unter Verwendung mehrer biometrischer Algorithmen bei nur einer Modalität,
- multiinstanziell durch Nutzung einer Modalität aber zweier Instanzen (z. B. zwei Finger)
- multisensorisch, also mit mehreren Sensoren die selbe Modalität messen (z. B. Infrarot und 3D-Scanning des Gesichtes)

zur Erfassung biometrischer Merkmale

Durch die Fusion der Werte aus mehreren Modalitäten, Algorithmen, Instanzen oder Sensoren wird die gemeinsame Prüfung der zusammengeführten Ergebnisse herbeigeführt.

Erkennung von Herzsignalen
Roland Sassen, thinsia, www.thinsia.com/products/heartbeat-id.html



Letztlich forsche er, wie mit kombinierten EKG-Werten des Herzens der signifikante „Herzton" herausgefiltert werden kann, der bei jedem Menschen eindeutig sei. Er setze bei der Forschung und Entwicklung auf einen etwa Chip-großen, berührungslosen EKG-Scanner zur Vermessung des Herzens. Aus dem Plenum der Präsentation kritisierten wir, dass bei dieser Technik auch personenbezogene medizinische Informationen anfallen, die missbräuchlich genutzt werden könnten. Die pragmatische sinngemäße Antwort, eine zusätzliche medizinische Früherkennung könne den Betroffenen nicht schaden, machte deutlich, dass der Schutz personenbezogener Daten manches Mal zu leichtfertig dem wissenschaftlichen und wirtschaftlichen Zielen untergeordnet werden.

Innenohr-Biometrie: Ein weiteres Forschungsprojekt wurde beispielsweise von Gary Garcia von Philips Research präsentiert. Es befasst sich mit der Analyse des Echos, das vom menschlichen Ohr reflektiert wird, nachdem in das Ohr zuvor eine Beschallung geschickt wurde. Dabei wird davon ausgegangen, dass dieses Echo jedem Menschen individuell und eindeutig zugeordnet werden könne. Der Ton wird von einem Sender direkt in das Ohr geleitet, mit einem Empfängermikrofon wird das Echo aus dem Gehörgang aufgenommen. Die akustische Vermessung soll eine Erkennungsgenauigkeit aufweisen, die dem Fingerabdruck ähnelt. Die Live-Demonstration zeigte die Funktionstüchtigkeit. Diese Technik soll mit handelsüblichen Mikrofon- und Kopfhörerbauteilen zum Beispiel in ein Mobiltelefon integrierbar sein, um z. B. ein Handy oder einen MP3-Player mit Zugangsschutz auszustatten.
Fraglich ist hier ebenfalls, wie die informationelle Selbstbestimmung des Menschen wirksam sichergestellt werden kann, wenn Gerätetechniken kombiniert werden, deren Funktionsweise die Schutzziele der personenbezogenen Daten nicht erfüllen. Das trifft beispielsweise auf die Sicherheitslücken bei der Bluetooth-Technik von mobilen Geräten zu. (vgl. dazu Kapitel „Funknetze – die rasante Entwicklung geht weiter"). Das Datenschutzniveau und die IT-Sicherheit bei kombinierten Technikkomponenten weisen zumeist nur ein Sicherheitsniveau auf, das genau der schwächsten Stelle entspricht.

Risiken

Eine absolute Erkennungsgenauigkeit bei biometrischen Verfahren ist nicht gewährleistet. Zudem verändern sich die meisten biometrischen Merkmale schon auf Grund des natürlichen Alterungsprozesses der betreffenden Person. Dieses Grundproblem stellt die Authentizität personenbezogener Daten bereits grundsätzlich in Frage.
Meist finden biometrische Verfahren bisher Anwendung im nicht-öffentlichen Bereich als Zugangs- oder Zutrittskontrolle. Denkbar sind sie aber auch im öffentlichen Bereich, insbesondere im Bereich der inneren Sicherheit.
Risiken beim Einsatz biometrischer Verfahren ergeben sich grundsätzlich immer dann, wenn eine willentliche Beeinflussbarkeit durch den Nutzer nicht mehr gewährleistet ist. Die passiven Merkmale lassen sich möglicherweise auch ohne Zutun des Betroffenen und unbemerkt erfassen, wie dies klassischerweise bei der Gesichtserkennung durch Videokameras denkbar ist. Je kleiner elektronische

Bauteile werden, desto unbemerkter können sie im Betrieb bleiben. Durch die Gefahr automatisierter Identifikation ohne Kenntnis der Betroffenen sind auch Bewegungsprofile erstellbar.
Auch ein grundsätzliches Problem ist für alle Verfahren typisch und damit ein Grundrisiko: Eine rein theoretische Abschätzung der Sicherheit, wie man sie aus der Kryptographie oder der Diskussion um die PIN (Persönliche Identifikations Nummer) kennt, gibt es in der Biometrie nicht. Das führt dazu, dass eine klare Einordnung der Zuverlässigkeit der Verfahren nicht möglich ist. Es bleiben Risiken, die auch von den herkömmlichen, manuellen Verfahren her – etwa durch Irrtümer, Verwechslungen, Ungenauigkeiten, subjektive Wahrnehmung – bekannt sind. Möglich sind Vergleichsansätze über die Fehlerraten bei falscher Erkennung oder falscher Zurückweisung. Sie basieren auf Mittelwerten und sollen die Feineinstellungen der Verfahrenstechnik überprüfbar machen.

Grundforderungen für Biometrische Verfahren

Bei der technischen Ausgestaltung biometrischer Verfahren ist insbesondere darauf zu achten, dass Daten im Besitz des Betroffenen zu halten sind und auf zentrale Speicherung zu verzichten ist und der ausschließliche Einsatz mittels mathematischer Komprimate in Erwägung zu ziehen ist, um den Zugang zu überschießenden Informationen aus Rohdaten und einen eventuellen Missbrauch zu vermeiden (z. B. medizinische Rückschlüsse aus Informationen zum Augenhintergrund bei der Retina-Erkennung).

Einführung biometrischer Ausweisdokumente

Die Terrorismusbekämpfung hat biometrische Verfahren zunehmend als Mittel zur sicheren Identifikation von Personen interessant werden lassen. Inzwischen ist die Speicherung biometrischer Merkmale in Personalpapieren (ePass – elektronischer Reisepass) Realität geworden.
Die notwendigen Sicherheitsmaßnahmen, die Befürchtung von Datenmissbrauch und zentralen Datensammlungen gaben und geben noch immer Zündstoff zur Diskussion über die technischen und organisatorischen Rahmenbedingungen, die die informationelle Selbstbestimmung schützen müssen und können.
Im Jahre 2005 hatte ich ein Projekt „Biometrie in Ausweispapieren – Entwicklung praxisorientierter Leitlinien am Beispiel von Werksausweisen“ geplant, das die datenschutzrechtliche Begleitung der Einführung solcher Verfahren zum Inhalt hatte. Da der Projektpartner diese Aktivität eingestellt hatte, war die Projektierung in meiner Dienststelle bisher ausgeblieben.
Da jedoch weiterhin Bedarf besteht, Praxiserfahrungen hinsichtlich der datenschutzrechtlichen Anforderungen an den Einsatz von biometrischen Verfahren zu sammeln und anschließend in geeigneten Handlungsempfehlungen so aufzubereiten, dass eine praxisorientierte Arbeitshilfe zur Verfügung steht, wurde die Thematik als ein datenschutzrechtlicher Handlungsschwerpunkt fortgeführt. Durch informelle Zusammenarbeit mit TeleTrusT Deutschland e. V. und die Mitgliedschaft im CAST-Forum (heute CAST e. V.) wurden dafür kompetente Diskussionspartner aus Forschung, Entwicklung und Wirtschaft gefunden. Beispielsweise bei der Erarbeitung eines “Kriterienkataloges zur Vergleichbarkeit

In einer **Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder** positionierten wir uns bereits am 1. Juni 2005 zur „Einführung biometrischer Ausweisdokumente“
Download unter http://www.sachsen-anhalt.de/LPSA/index.php?id=20274

Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren: http://www.teletrust.de/fileadmin/files/publikationen/KritKat-3_final.pdf

„Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme" http://www.teletrust.de/fileadmin/files/ag6/ag6_ak-recht_orientg-betriebsvbg-biometrie_1.2.pdf

biometrischer Verfahren" (siehe Kasten) mit einem eigenen Datenschutzkapitel sowie einer „Orientierungshilfe für eine Betriebsvereinbarung beim Einsatz biometrischer Systeme" (siehe Kasten) hatten wir Gelegenheit, in der Arbeitsgruppe 6 „Biometrische Identifikationsverfahren" und dem Unterarbeitskreis Recht des TeleTrusT Deutschland e. V. mitzuarbeiten, datenschutzrechtliche Diskussionen zu führen und Impulse zu geben. TeleTrusT hat sich zum Ziel gesetzt, hier einen Erfahrungsaustausch über biometrische Verfahren zu organisieren und daraus resultierend ihren vertrauenswürdigen Einsatz zu fördern.
Eine intensive Recherche technischer Weiterentwicklungen und des Marktgeschehens wurde im Berichtszeitraum fortlaufend durchgeführt und wird auch weiterhin erfolgen.

Funkchips – die kleine Invasion der Konsumentenwelt

RFID (Radio-Frequency-Identification) ist ein Verfahren, bei dem miniaturisierte IT-Systeme **(RFID-Chips, RFID-Tags)** über Funksignale mit geeigneten Lesegeräten kommunizieren. Dabei kann je nach Ausstattung des RFID-Tags die Übertragungsreichweite zwischen wenigen Zentimetern und mehreren Metern liegen. Und auch die auf dem RFID-Tag gespeicherten Datenmengen können zwischen einem einfachen Bestätigungssignal (Diebstahlsicherung an Waren) über eine Warennummer bis hin zu Personendaten in einem Personalausweis oder auf einer Kundenkarte variieren.

Die Fragen der Entwicklung und der Einsatzfelder einer elementaren Basistechnologie macht seit ein paar Jahren Furore: Die Rede ist von den RFID-Chips (Radio Frequence Identification).
Die Grundlagentechnologie wird als Bestandteil zahlreicher Verfahrens- und Anwendungsentwicklungen prognostiziert und gewinnt langsam zunehmend auch für öffentliche Bereiche Bedeutung. Es ist zu erwarten, dass neben den bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln und anderen Konsumgütern künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein. Dieses Ziel wird inzwischen nachhaltig verfolgt. Sofern ihre Funktionsfähigkeit nicht deaktiviert wird, sind bei dieser Verbreitung diese RFID-Chips unbemerkt elektronisch auslesbar. Damit wäre der jeweils dazugehörige Artikel sowie damit auch die diesen Gegenstand bei sich tragende Person identifizierbar. Hieraus sind durchaus Rückschlüsse auf Eigentums- und Besitzverhältnisse ziehbar.
Die flächendeckende Einführung dieser Kennzeichnung birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden zusammengeführt werden. In der Praxis ist dies in der Regel auch ohne deren Wissen und Wollen möglich, aber meines Erachtens nicht zulässig. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht, die für verschiedenste Zwecke, vor allem für die Kundenbindung und äußerst gezielte Bewerbung von Produkten geeignet wären.
Ich halte daher die Beachtung der datenschutzrechtlichen Grundprinzipien Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz für das dringendste Gebot für die Einführung dieser Technik. Diesen Prinzipien lässt sich nur Geltung verschaffen, wenn die treibenden Kräfte ihre Gültigkeit und Umsetzung auch beachten. Daher sind Hersteller und Anwender im Handels- und Dienstleistungssektor aufgerufen, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen.
Der Handlungsschwerpunkt RFID, der für mich auch 2005 bereits bestand, sollte in 2006 um ein konkretes Anwendungsfeld ergänzt werden. Das Projekt „An-

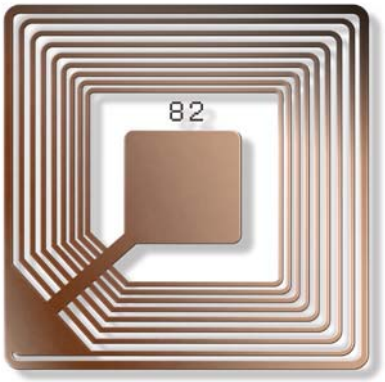
wendung von RFID-Tags im Bibliotheksbereich der TU Clausthal“ wurde von uns Anfang 2006 kooperierend begleitet und teils mitgestaltet. Anhand konkreter Planung mit dem Kooperationspartner in der Universitätsbibliothek Clausthal sollte ein Konzept zur datenschutzgerechten Ausgestaltung erarbeitet werden, das den beispielhaften Umgang mit der Technologie am praktischen Anwendungsfeld der Buchetikettierung mit RFID-Chips (Tags) transparent aufzeigt. Dabei wurde von uns vor Ort eine Bestandsaufnahme vorgenommen, bei der der geplante Nutzen bei der Buchentleihe und Rückgabe sowie des Bestandes untersucht und auf die datenschutzrechtlichen Risiken insbesondere bei den Abläufen und hinsichtlich der Datenstrukturen analysiert wurde. In einer Handlungsempfehlung wurden dem Anwender Hinweise gegeben, welche Maßnahmen die Ausgestaltung des Verfahrens beinhalten sollten. Durch die Arbeit im AK Technik ist auch in diesem Themenbereich gewährleistet, dass es zu einem bundesweiten Erfahrungsaustausch und Abstimmungsprozessen kommt.

Mit der **Firma Metro** (verantwortlich für den METRO Group Future Store und METRO Group RFID Innovation Center in Neuss) sowie dem Interessenverband Informationsforum RFID e. V. in Berlin wurden von uns zeitweilig intensive Kontakte gepflegt. Im Januar 2006 hatten wir Gelegenheit, das METRO Group RFID Innovation Center in Neuss zu besichtigen, die Testumgebungen vor Ort kennenzulernen und mit Vertretern der Firma über die Chancen und Risiken einer flächendeckenden Nutzung der Chips zu sprechen. Dabei konzentrierten wir uns auf die Anwendungsszenarien des Einzelhandels. Es bleibt hier insbesondere die Forderung nach der Entscheidungsfreiheit, die RFID-Tags zu deaktivieren oder zu entfernen, im Raum. Es soll gerade in der Hand des Kunden liegen, ob die RFID-Identifikation seines Artikels frei ausgelesen werden kann oder nicht. In der Praxis dürfte diese Option bei derzeitigem Stand der Technik aufgrund zeitraubender Einzelprozeduren vor einem „Deaktivator“ leider kaum dazu führen, dass die Konsumenten davon dauerhaft Gebrauch machen. Hier sind Verbesserungen in der Handhabung erforderlich. Das Interesse des Einzelhandels steht dem Deaktivieren der Chips durchaus entgegen, denn Funktionen – etwa im Garantiebereich – sind fortan nach dem Deaktivieren nicht mehr verfügbar. Die Geschäftsprozesse zu beschleunigen ist aber ebenfalls ein Kostensenkungsziel des Handels.

METRO Group RFID Innovation Center
www.future-store.org/servlet/PB/menu/1007062_l1/index.html

Interessenverband Informationsforum RFID e.V.
www.info-rfid.de

Eine weitere Problematik ist nicht zu unterschätzen: Die Miniaturisierung der Tags (derzeit bereits ein Quadratmillimeter möglich) führt dazu, dass ihre Existenz übersehen werden könnte. Daher ist eine Kennzeichnung unbedingt erforderlich.



Computerfachwelt spricht „RFID“: Schwerpunktthema auf der CeBIT 2006

Auf der CeBIT 2006, der größten IT-Fachmesse der Welt in Hannover, auf der wir unseren Datenschutztag durchgeführt hatten, hatten wir mit einer Podiumsveranstaltung das Thema RFID-Chips zum zentralen Thema erklärt. Vertreter von Wirtschaft, Wissenschaft, Interessenverbänden und des Verbraucherschutzes wurden in einer Fachpodiumsdiskussion mit den technischen und materiellrechtlichen Datenschutzfragen konfrontiert. Die Technologien und die Anwendungsfelder von RFID stellten auch einen der Hauptschwerpunkte auf der CeBIT

für die Aussteller dar. Das Medienecho war – auch im Hinblick auf die datenschutzrechtlichen Bewertungen – entsprechend sehr hoch.

Firma PCO (Tochterunternehmen der Hellmann Worldwide Logistics) www.pco-online.de/magazin/artikel.php?artikel=368&type=2&menuid=179&topmenu=2

Zu einer Veranstaltung in der Logistikbranche in Osnabrück wurden wir im Frühjahr 2006 gebeten, die datenschutzrechtliche Bewertung im Umgang mit den Funkchips zu präsentieren. Auch hier, direkt im Anwendungsbereich der RFID-Technik, zeigte sich ausgiebiger Diskussionsbedarf in und mit der Wirtschaft und ihren Verbänden über die Beurteilung der technischen und organisatorischen Maßnahmen zur datenschutzgerechten Ausgestaltung bei der Anwendung.

Über die niedersächsischen Grenzen hinweg

Im Arbeitskreis „Technische und organisatorische Datenschutzfragen" wurde Ende 2006 eine Orientierungshilfe[1] erarbeitet, die die Technologie und Anwendungsfelder der RFID-Tags aus datenschutzrechtlicher Sicht betrachtet. Hier sind wir übereinstimmend zu der Ansicht gelangt, dass RFID in vielen Fällen datenschutzrechtliche Risiken und Nebenwirkungen birgt, die individuell und in ihren gesamtgesellschaftlichen Folgen nicht unterschätzt werden dürfen.

In einer Entschließung hatten wir in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder kurz zuvor im Herbst 2006 verbindliche Regelungen für den Einsatz von RFID-Technologien gefordert, um das Risikopotential für die Gesellschaft kontrollierbar zu halten zu können.[2]

Das Bundesverfassungsgericht hat bereits mehrfach den Gesetzgeber darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Zum Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu RFID zu berücksichtigen:

- Transparenz
  Alle Betroffenen müssen umfassend über Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.
- Kennzeichnungspflicht
  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.
- Keine heimliche Profilbildung
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegen-

[1] **Orientierungshilfe „Datenschutzgerechter Einsatz von RFID"** des Arbeitskreises „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom vom 14.12.2006; Quelle/Download: <http://www.bfdi.bund.de/nn_530436/SharedDocs/Publikationen/Orientierungshilfen/OH__RFID.html

[2] **Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder** vom 26.–27.10.2006 in Naumburg "Verbindliche Regelungen für den Einsatz von RFID-Technologien" <http://www.sachsen-anhalt.de/LPSA/index.php?id=20563>

stände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

- Vermeidung der unbefugten Kenntnisnahme
  Das unbefugte Auslesen der gespeicherten Daten muss durch geeignete Maßnahmen – beispielsweise durch Verschlüsselung – bei ihrer Speicherung und Übertragung unterbunden werden.
- Deaktivierung
  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit für Kunden bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen. Das gilt insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Allgegenwärtigkeit von Computern bergen Risiken für die informationelle Selbstbestimmung

Die Allgegenwärtigkeit von Computern, anderer Mikroprozessor gesteuerter Geräte und der heutigen und künftigen RFID-Chips hat inzwischen den Status futuristischer Fantasieszenarien verlassen.

Schon im Jahr 2000 kamen laut Erhebungen der Pentagon-Forschungseinrichtung DARPA 8 Milliarden Mikroprozessoren zum Einsatz. 98 Prozent der Prozessoren arbeiteten in eingebetteten Systemen (Embedded Systems), lediglich 2 Prozent in Anwendungen wie dem klassischen PC. (Heise Online, 22.09.2004, www.heise.de/newsticker/meldung/51363). Die Europäische Union (EU-Kommission) förderte den Bereich in ihrem 6. Rahmenprogramm mit insgesamt 3,63 Milliarden Euro mit stark steigender Tendenz.

Das ist jedoch nur der Anfang: Es gibt konkrete Vorstellungen und Pläne, diesen angestrebten Zustand des so genannten „ubiquitären Computing“ (siehe Erklärung im Kasten) so zu gestalten, dass nicht mehr der Mensch seinem Willen entsprechend die Technik nutzt, sondern dass die Geräte die Funk-Kommunikation untereinander selbständig aufnehmen, um eine vernetzte Funktionalität im Dienste des Menschen sicherzustellen.

Hier trägt die Miniaturisierung elektronischer Bauteile und das Einbauen in Alltagsgegenstände (so genannte embedded Systems) erheblich zur unmerklichen Funktionalität bei. An dieser Stelle kommt der Chiptechnologie plötzlich eine eigenständige Rolle zu, die zwar unzählige sinnvolle Funktionen und Vorteile für Sicherheit und Komfort im Alltag bietet, die jedoch andererseits auch sehr bedenklich wird. Das Bild des Kühlschrankes, der selbständig das Ablaufdatum eines Lebensmittels oder das Fehlen des Lieblingsproduktes erkennt und per Kommunikationsleitung oder per Funk den Nachschub bestellt, ist inzwischen ein populäres Beispiel geworden.

Ein weiteres Problem ist die Feststellung der Verantwortlichkeit für die Funktionen des Gerätezusammenspiels. Wer ist dann die von den Datenschutzgesetzen definierte „Daten verarbeitende Stelle“? Die klassische Datenübermittlung ist nur schwer auf das Bild eng vermaschter, zahlloser Einzelkomponenten übertragbar. Klar trennbar ist kaum noch ein Kommunikationsprozess zu identifizie-

Ubiquitäres Computing (engl. **Ubiquitous Computing, „UbiComp“**) nennt man die Allgegenwärtigkeit von Mikroprozessor gesteuerten Vorgängen und elektronischer Kommunikation zwischen Personen aber auch zwischen Geräten im menschlichen Alltag und Berufsleben. Computer werden in nahezu alle Geräte eingebettet. Durch zusätzliche Funknetze und Mobilität des Technikeinsatzes kann eine neue Qualität der Funktionalitäten und ihrer Kombination untereinander erreicht werden. Die ständige mobile Veränderung der Bestandteile sowie deren Fähigkeit zur Selbstkonfiguration und –verwaltung verleiht dem Gesamtsystem eine enorme Dynamik.

Der Begriff **Pervasive Computing (PvC)** beschreibt einen ähnlichen Umstand aus einem industriell geprägten Blickwinkel. Er bedeutet Durchdringung, hier also durch Computer und die flächige Vernetzung des Alltags durch den Einsatz computergesteuerter Gegenstände.

Ambient Intelligence (AmbI) heißt ‚intelligente Umgebung‘. Das bedeutet, dass die Alltagsgegenstände, die den Menschen umgeben, sich adaptieren und sensitiv auf dessen Anwesenheit und die anderer Objekte reagiert und dabei für den Menschen in vielfältiger Weise Dienste erbringt. Die Nutzung der Computerleistung soll dabei nicht mehr Aufmerksamkeit erfordern, als alle anderen

ren. Gleichwohl sind sensible Lebensgewohnheiten oder Einzelinformationen zu Personen konstruierbar oder rekonstruierbar. Eine Profilbildung erhält ganz neue technische Werkzeuge und ist aufgrund erheblich größerer Datenmengen wesentlich aussagekräftiger als herkömmliche Einzelinstallationen. Die Privatsphäre wäre in einer nie da gewesenen Dauerhaftigkeit und Intensität beobachtbar, wodurch sie faktisch aufgehoben sein könnte.

Grenzen des Eigenlebens bestimmen

Die Frage, wieviel Eigenständigkeit von Geräten erwünscht ist, hängt von der Vorstellung des Menschen ab. Es muss aus meiner Sicht immer in der Entscheidungshoheit des Einzelnen bleiben, welche der ihn betreffenden Informations- und Kommunikationsprozesse wann und mit wem stattzufinden oder zu unterbleiben haben. Das gilt umso mehr für die personenbezogenen Informationen. Die Bestimmung der Grenzen ist hier verfassungsrechtlich nur durch Gesetze möglich.

Die ubiquitäre Computerwelt droht, mit diesem Grundsatz prinzipbedingt zu brechen. Die Entwicklung ist angetreten, das menschliche Lebensumfeld nachhaltig zu verändern. Die Bequemlichkeit in einer computergesteuerten Konsumentenwelt macht es bekanntlich allzu leicht, sich den Automatismen hinzugeben und dabei die Selbstbestimmung sukzessive aufzugeben. Schon heute ist – insbesondere im Zusammenhang mit Videotechnik – sehr oft der einfache Satz „Ich habe nichts zu verbergen" zu hören. Offenkundig verkennen noch viele, dass es hier nicht um das – nachvollziehbare – Vertrauen gegenüber einer einzelnen Person geht, sondern um das völlig unterschätzte Risiko, seine Daten für Manipulation, Missbrauch und Auswertung einer unbegrenzten Zahl potentieller Täter freiwillig auszuhändigen. Die Privatsphäre muss regelmäßig unbehelligt und gewahrt bleiben, Informationsverarbeitung darf sich nur auf berechtigte Ausnahmen und Einwilligungsfälle beschränken. Hier wird bei unmäßiger Ausweitung von Registrierung, Spurverfolgung (Tracking), Datenverarbeitung und -austausch jedoch dieser Grundsatz auf den Kopf gestellt. Eine Aushöhlung der informationellen Selbstbestimmung, aber auch das Nichtwahrnehmen eigener Interessen aufgrund fehlender Kenntnis zur Risikoeinschätzung ist datenschutzrechtlich sehr bedenklich.

Während die Steuerung ganzer Logistikketten von der Produktion bis zum Einzelhandel durch den Einsatz von RFID-Chips für den Datenschutz problemlos ist, nimmt die Zahl der Einsatzbereiche zu, in denen personenbeziehbare Informationen Gegenstand der Chipsteuerung werden. Militär, Museen, Bibliotheken, Krankenhäuser, Automobilhersteller, Handel, öffentlicher Personennahverkehr und sogar Schulen setzen auf die RFID-Technologie zu Informations- und Überwachungszwecken. Bei der Tierkennzeichnung, für die Zeitnahme bei Marathonläufen, in Reisepässen und auf Eintrittskarten für Großveranstaltungen finden RFID-Tags ebenfalls Verwendung. Selbst über die Integration in Euroscheine wird bereits diskutiert.

Alltagsgegenstände. Das Konzept unterscheidet stationäre, nomadisierende und autonome Geräte. Es handelt sich um ein technologisches Paradigma. Das europäische Forschungsprogramm „Information Society Technologies" hat mit dieser Definition einen EU-Weg für Wirtschaft und Technologie vorgezeichnet. AmbI konzentriert sich auf die Entwicklung von Architekturen und Anwendungen und weniger auf die der technischen Grundbausteine. Die Ziele sind ansonsten vergleichbar mit denen der US-amerikanischen Forschung, → Ubiquitous Computing (allgegenwärtige Rechner), der sich jedoch an der Hardware orientiert. Auch der Ansatz der Industrie namens →„Pervasive Computing" (PvC) ähnelt AmbI.

Next Generation Media ist der Terminus der Bundesregierung als Innovationsinitiative, der die Begriffe →UbiComp, →AmbI und →PvC zusammengefasst. Forschungsziel ist die massive Vernetzung von Sensoren, Funkkommunikation und Prozessoren für die alltäglichen Erleichterungen, etwa dem intelligenten Haus, in dem die Steuerung von Wärme, Technik, Fenster, Rollläden durch mobile Computer erfolgt oder Sensornetze zur Steuerung der Infrastruktur wie Brand- und Katastrophenschutz, Erdbebenfrühwarnung, Verkehrsflusskontrolle.
Ein spezieller Forschungsbereich ist das sogenannte **Wearable Computing** (tragbare Rechner). Hier geht es darum, in die Bekleidung IT-Komponenten zu integrieren, die sensorisch Umgebungsbedingungen messen und mitteilen, Entertainment ohne Kabelsalat anbieten (MP3) oder Funkkommunikation bereitstellen.

Mit **Smart Dust** werden drahtlose Sensornetze (wireless sensor network, auch intelligenter Staub genannt) bezeichnet. Es ist ein Netzwerk von kleinsten drahtlos kommunizierenden Computern, jeweils bestehend aus einem Prozessor und einem Datenspeicher oder in Form eines RFID-Tags. Diese Sensorknoten sind fähig, sich selbst in einem Ad-hoc-Netz – also ohne feste Infrastruktur – zu organisieren und benachbarten Kontakt zueinander aufzubauen, um letztlich ihre Umgebung arbeitsteilig zu überwachen. Diese mikroelektronischen

Pervasive Computing

Ähnlich der Idee des ubiquitären Computing ist der von der Industrie geprägte Ansatz des Pervasive Computing (PvC). Das BSI kam zum PvC in seiner Studie 2006 (Quelle: [BSI-Studie], Siehe Kasten) zu folgenden Kernaussagen des Datenschutzes:

„Noch mehr als bei anderen IT-Systemen ist […] der Datenschutz im Pervasive Computing eine wesentliche Voraussetzung für die Wahrung der informationellen Selbstbestimmung. Auch hier gelten die vorhandenen Datenschutzprinzipien und -regelungen. ([BSI-Studie], a. a. O., Kap. 2.6) Diese gewinnen gegenüber herkömmlichen Informationssystemen noch einmal an Bedeutung. Die große Anzahl an intelligenten Gegenständen und ihre spontane Vernetzung erschwert die Beherrschbarkeit des Gesamtsystems. Zudem wird für den Nutzer die Abhängigkeit von einer Vielzahl von für ihn nur sehr schwer zu durchschauenden Hintergrundprozessen erhöht […]. Die verteilt erbrachten Dienste erschweren es, die Zusammenhänge zwischen einer Aktion im Pervasive Computing und ihren Folgen hinsichtlich der Weitergabe und Verarbeitung der eigenen Daten zu erkennen." ([BSI-Studie], a. a. O., Kap. 5.6)

Diese Aussagen des BSI und einige mehr in der Studie decken sich im Kern mit meiner Einschätzung zu dem Themenkomplex UbiComp und PvC. Es wird in Zukunft noch sehr viel kritischer der Fortgang der Entwicklungen betrachtet werden müssen. Es gilt, den Forderungen zur Beachtung der Privatsphäre einerseits Geltung zu verschaffen und andererseits die beteiligten Forscher, Hersteller, Konsumenten aber auch politische Entscheider für ihre hohe Verantwortung zu sensibilisieren. Das Ziel lautet auch hier, das Recht auf informationelle Selbstbestimmung nicht zu opfern, um Platz für eine vermeintliche Verbesserung zu schaffen.

Videotechnologien

Videotechnik eröffnet heute durch Preisverfall und technische Weiterentwicklungen neue Dimensionen der Anwendungen, der Funktionalität, der Qualität und der Aufbereitungsmöglichkeiten. Sie weist einen hohen innovativen Wandel auf und erschließt sich ständig neue Anwendungsfelder. Diese neuen Dimensionen bieten allerdings auch die Möglichkeit, ein sehr viel höheres Maß an Überwachungstiefe und Flächendeckung zu erzielen.

Aufgrund der Fortentwicklung von Detektions- und Erkennungssoftware sowie biometrischer Funktionalitäten kommt eine völlig neuartige Qualität der Überwachung zustande. Dadurch sind immer mehr Menschen einer immer stärkeren Beobachtung ausgesetzt. Zudem ist durch kombinierte Erkennungstechnik zunehmend die Privatsphäre gefährdet.

Die Vorteile digitaler Kameras in funktionaler Hinsicht bestehen in deren besserer Vernetzbarkeit und in ihrer geringeren Größe. Das führt dazu, dass im zunehmenden Maß diese viel kleineren Kameras leicht unbemerkt installiert werden und deren Bilder auch in einer größeren Anzahl über Internetverbindungen an entfernte Leitstände übermittelt werden können. Die digitale Videoüberwachungstechnik ist hier im Vormarsch, 2005 waren schon etwa 20 % Marktanteil gegenüber den analogen Kameras zu verzeichnen.

Bausteine können derzeit bis zu einer Miniaturisierung von 1 mm gebaut werden.
Die Einsatzszenarien sind vielseitig, die Zahl der Bauarten ebenfalls. Anwendungen existieren bisher im Versuch. Erste Entwicklungen sind am Markt verfügbar. Forschungsfeld ist vor allem das Energiemanagement für lange Ruhepausen und geeignete Netzprotokolle, die die erforderliche autonome Kommunikation handhabbar machen.

Einen völlig neuartigen Zugang zu der zustande kommenden Informationsdichte könnte mit der **TAG-Methode** erlangt werden. TAG bedeutet **Tiny Aggregation** und nutzt das Sensornetz wie eine virtuelle Datenbank. Mit Hilfe einer Datenbankabfragesprache könnten die Informationen über einen Knoten abgefragt und zu Informationseinheiten aggregiert werden.

Quelle **[BSI-Studie]**, Studie im Auftrag und Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Kooperation von VDI/VDE Innovation und Technik GmbH, Fraunhofer Institut für sichere Informationstechnologie (Fhg SIT) und Sun Microsystems GmbH, November 2006: „Pervasive Computing: Entwicklungen und Auswirkungen"

Studie des ULD und der Humboldt-Universität Berlin: **„Technikfolgenabschätzung Ubiquitäres Computing und informationelle Selbstbestimmung (TAUCIS)"**, im Auftrag des Bundesministeriums für Bildung und Forschung, Juli 2006, insbesondere Kapitel 6. Datenschutzrechtliche Risiken des Ubiquitous Computing und rechtliche Möglichkeiten des Risikomanagements und Kap. 9.2 Anforderungen aus dem und an das Datenschutzrecht https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf

Gesellschaft für Informatik (GI) e.V. zu : http://www.gi-ev.de/presse/pressearchiv/presse-mitteilungen-der-gi-im-jahr-2004/pressemitteilung-vom-22-september-2004/

Fraunhoferinstitut IGD – Ambient Intelligence Lab: http://www.igd.fhg.de/igd-a1/projects/ami-lab/index.html

Digitale Videografie – aktuelle Standards:
Bei den **Bilddatenformaten** gelten MPEG und MJPEG als Standard. Zu erwarten ist die Zusammenführung von Bild- und Tonübertragung in einem Standard, um Bild (insbesondere Lippenbewegungen) und Ton zu synchronisieren.
Bei der **Datenspeicherung** ist das Überschreiben aufgezeichneter Daten nach einer definierten Zeit (Endlosschleife) Stand der Technik.
Stark verbessert hat sich inzwischen die **Navigation** durch Kamerasysteme und Bildspeicher. Insbesondere ist die Auswahl einer geeigneten Kamera aus einem System, die Bilder von einem gegebenen Standort liefert, einfacher geworden. Das führt zu effizienteren Überwachungserfolgen.

Das Berechtigungsmanagement
Moderne Videoüberwachungssysteme bieten mehrstufige Berechtigungskonzepte, die auch Realisierung des Vier-Augen-Prinzips bei bestimmten Zugriffen gestatten. Das stellt ein wichtiges Merkmal dar, um durch transparente organisatorische Regelungen und technische Administration unberechtigte Zugriffe auf die Daten und Systeme zu verhindern.

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten von Bund und Ländern (AK Technik) hat sich bereits 2005 mit der ersten Version eines Schutzprofils „Video" befasst. Dieses Schutzprofil wurde vom Bundesbeauftragten für den Datenschutz und Informationsfreiheit sowie der datenschutz nord GmbH erstellt. Die erste Version war in zwei Varianten unterteilt: Videoanlagen mit sicheren und mit unsicheren Übertragungswegen. Im Rahmen der Beratung ist auch der Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (ZVEI) in Person und Funktion des Vorsitzenden des Fachkreises Videosysteme im Fachverband Sicherheitssysteme zu einer fachlichen Diskussion eingeladen worden. Dabei stand die Frage im Mittelpunkt, inwieweit die Videotechnikbranche den Ansatz mitträgt, die Videotechnik einer gewissen Standardisierung im Interesse datenschutzfreundlicher Lösungen zu unterziehen. Die Branchenvertreter ließen eine ablehnende Haltung gegenüber Regulierungen und einer aus Ihrer Sicht hinderlichen etwaigen datenschutzrechtlichen Zertifizierung oder eines Gütesiegelverfahrens für Videotechnik erkennen. Vielmehr wird seitens der Branche auf die Innovationskraft und Selbstregulierung der Wirtschaft vertraut.
Es ist allerdings überwiegende Meinung der Mitglieder des AK Technik und auch unsere Auffassung gewesen, dass es definierte technische Standards geben muss, um Hilfestellungen für eine datenschutzgerechte Ausgestaltung der Planung, der Installation und des Betriebes von Videoüberwachungsanlagen sowie der digitalen Verarbeitung der Videos zu geben. Eine Option zur Zertifizierung wäre insofern hilfreich, die Produkte gegen diese Vorgaben zu prüfen, die Akzeptanz für und das Vertrauen in die Technik fördern zu können. Nebenbei würde sich dies sogar wettbewerbsfördernd auswirken, weil mit einer solchen Zertifizierung für ein datenschutzkonformes Konzept oder Produkt geworben werden könnte. Dabei ist klar, dass die Prüfung eines Produktes auf Datenschutz oder IT-Sicherheit nicht automatisch dazu führt, dass es auch datenschutzgerecht eingesetzt wird. Viele Auftraggeber sind jedoch fachlich den Auftragnehmern bei technischen Verhandlungen im IT-Bereich oft nicht hinreichend gewachsen. Den Auftraggebern fehlt häufig technisches Detailwissen, um die eigenen Anforderungen vollständig und sachgerecht zu definieren. Hier kann das Schutzprofil ansetzen, indem wichtige Prüffragen generalisierend vorgegeben werden.

„Common Criteria Protection Profile" – Software zur Verarbeitung von personenbezogenen Bilddaten; BSI-PP-0023-2007Version 2.0" vom 15.01.2007, www.bsi.bund.de/zertifiz/zert/reporte/PP0023b.pdf

Schutzprofil Video

Das BSI und der BfDI haben am 15. Januar 2007 eine neue Version des Schutzprofils für datenschutzfreundliche Videoüberwachungsanlagen herausgegeben. (Siehe Kasten). Dieses auf den Common Criteria Vers 2.3 basierende Schutzprofil beinhaltet die Mindestanforderungen, die an die Software zur Verarbeitung (Erheben, Speichern, Löschen und Nutzen) von personenbezogenen Bilddaten gestellt werden, um einerseits den datenschutzrechtlichen Bestimmungen zu genügen und andererseits eine anwenderfreundliche Bedienung der IT-Sicherheit moderner Videoüberwachungsanlagen zu ermöglichen.
Die hier charakterisierte datenschutzkonforme Videoüberwachungsanlage kann Bilddaten von angeschlossenen Signalaufnahmekomponenten empfangen und auf Authentizität (Herkunft der Daten) prüfen. Einmal gespeicherte Bilddaten stehen unter der Kontrolle der Anlage, bis sie gemäß der maximalen Aufbe-

wahrungsfrist automatisch gelöscht werden. In dieser Zeit können über die Videoüberwachungsanlage nur registrierte Benutzer auf die Bilddaten zugreifen. Neben der Verarbeitung der Bilddaten ist die Videoüberwachungsanlage auch in der Lage, alle datenschutzrelevanten Benutzeraktionen zu protokollieren. Solche Anlagen schützen die Bilddaten erst nach dem Empfang. Die Umgebung der Videoüberwachungsanlage muss daher dafür sorgen, dass die Bilddaten vertraulich, integer und authentisch bei der Videoüberwachungsanlage ankommen.

Ich werde in meinem Zuständigkeitsbereich künftig darauf achten, dass bei Ausschreibungen der öffentlichen Verwaltung dieses Schutzprofil zugrunde gelegt wird, um die Förderung des Einsatzes datenschutzgerechter Technik sicherzustellen.

In einem von uns durchgeführten Workshop im Herbst 2005 hatten wir uns mit der für die Polizei interessanten Betrachtung der neuen Technologien und ihrer Anwendung beschäftigt. Dabei war es uns auch wichtig, die Sichtweise der Ermittlungsbehörden zu berücksichtigen, die uns seitens des Landeskriminalamtes Niedersachsen erläutert wurde.

Kfz-Datenspeicher

Autos fahren heute längst nicht mehr rein mechanisch. Die Elektronik ist wichtiger Bestandteil von Steuerungen geworden: Zündung, Einspritzung, Airbag, Abstandssensoren für Einparkhilfe und viele Zusätze mehr helfen, die Sicherheit und den Komfort der Fahrzeuge zu verbessern. Immer mehr Speicherbausteine werden in Autos eingebaut.

Für eine umfassende Fehlerdiagnose bei der Wartung in der Werkstatt werden Fehlerdaten gespeichert. Fraglich ist dabei, wer die Daten auslesen und auswerten kann. Auch die Frage, ob die Daten über Funkverbindungen an Server übertragen werden und wer dann den Zugriff darauf hat, stellt sich unter Umständen. Zweckbindung und Freiwilligkeit der Erhebung, Verarbeitung und Übermittlung sind hier sensibel zu untersuchen.

Der **Unfalldatenspeicher (UDS)** nimmt über Sensoren ständig verschiedene Daten aus dem Fahrzeugbetrieb auf, z. B. Geschwindigkeit, Fahrtrichtung, Beschleunigung in Längs- und Querrichtung, Status von Beleuchtung und Fahrtrichtungsanzeiger, Verzögerungs-/Bremstätigkeit). Die Daten werden für einige Minuten aufgezeichnet, bevor sie von neueren Daten überschrieben werden.

Versicherungen erproben schon heute den Einsatz von Speichern, die risikoarmes und risikofreudiges Fahrverhalten anhand gemessener Einzeldaten von Lenkung, Bremsen und Beschleunigungswerten speichern. Aus den Fahrgewohnheiten kann eine risikoabhängige Tarifierung berechnet werden. Unfalldaten können mit Unfalldatenspeichern (UDS) – ähnlich einer Blackbox mit Flugdatenschreiber – aufgezeichnet werden, um den Unfallhergang zu dokumentieren und die Daten zur Beweisführung heranzuziehen. Je mehr Informationen über derartige Zustände und Hergänge beim Autofahren vorliegen, desto aussagekräftiger könnte die Gesamtinformation über das Fahrverhalten oder sogar die Lebensumstände der Fahrer werden. Angereichert um die Informationen zu den jeweiligen Fahrtrouten und Standorten sowie Fahr- und Standzeiten über die satellitengestützten Navigationsdaten der immer beliebteren GPS-Navigationsgeräte ließe sich ein außerordentlich präzises Bewegungsprofil erzeugen. Auch wenn in Niedersachsen oder Deutschland bisher noch kein solch umfangreich kombiniertes Szenario bekannt geworden ist, so könnten alle genannten Einzelkomponenten durchaus schon heute die Bausteine für ein solches Einsatzfeld ergeben.

EU-Projekt VERONICA („Vehicle Event Recording based on Intelligent Crash Assessment"), Abschlussbericht (PDF) bei http://www.siemensvdo.com/aboutus/projects/veronica

In dem Projekt „VERONICA" (siehe Kasten) der Europäischen Union wurden bis Ende 2006 Entwicklungen von Ereignisdatenspeichern und Implementierung in eine Systemumgebung definiert. Es scheint, dass hier ein maximales Ausmaß der technisch machbaren Leistungsmerkmale an die Technologie definiert werden sollte. An dem Projekt-Konsortium sind große deutsche Firmen maßgeblich beteiligt gewesen.

Eine Arbeitsgruppe (AG) des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und des Düsseldorfer Kreises unter Federführung des hessischen Datenschutzbeauftragten, in der wir ebenfalls vertreten waren, hat im Auftrag des Düsseldorfer Kreises das Thema Fehler- und Unfalldatenspeicher behandelt und wird als Ergebnis ein gemeinsames Arbeitspapier zur Thematik erstellen. Die AG hat im Herbst 2006 begonnen, die technischen und rechtlichen Aspekte von Fahrzeugdatenspeichern, insbesondere von Fehler- und Unfalldatenspeichern in PKW zu untersuchen. Fraglich war, welche Personenbeziehbarkeit mit diesen Fahrzeugdatenspeichern verbunden ist, wer Eigentümer solcher Daten ist und in wessen tatsächlichem Besitz sich die Daten befinden: Zulieferer des Kfz-Herstellers, Hersteller, Werkstatt, Fahrzeughalter oder Fahrzeugführer? Ferner ist zu hinterfragen, ob es sich in der Praxis um wirklich freiwillige Speicherungen handelt. Von Interesse ist auch, ob Risiken für die Privatsphäre von Autofahrern, die Manipulierbarkeit der Speicherbausteine und die Integrität der Daten bestehen.

Die Ergebnisse der Arbeitsgruppe liegen inzwischen als für die Datenschutzbeauftragten von Bund und Ländern internes Arbeits- und Prüfpapier vor.

Die weitere Forschung, die Entwicklungen und die ökonomischen Geschäftsmodelle werden von uns weiterhin aufmerksam beobachtet werden.

ANHANG zum TB 2005/2006:
Neue Orientierungshilfe

Neue Orientierungshilfe zum Datenschutz

Orientierungshilfe zum Datenschutz für kommunale Mandatsträgerinnen und Mandatsträger

„Das Niedersächsische Datenschutzgesetz findet somit grundsätzlich auf meine Tätigkeit als Mandatsträger Anwendung! Es gibt aber eine Reihe von spezialgesetzlichen Regelungen, die vorrangig anzuwenden sind (§ 2 Abs. 6 NDSG). Dies sind Bestimmungen aus der NGO, zum Beispiel über das Verfahren bei Angelegenheiten, die der Geheimhaltung unterliegen (§ 5 Abs. 3 NGO) oder zur Amtsverschwiegenheit (§ 25 NGO). Zudem gibt es das Sozialgeheimnis nach § 35 des Sozialgesetzbuches (SGB I Allgemeiner Teil), das Steuergeheimnis nach § 30 der Abgabenordnung (AO), Regelungen des Niedersächsischen Meldegesetzes (NMG) zu Melderegisterauskünften (§§ 33, 34 NMG) oder spezielle Vorschriften zur Personaldatenverarbeitung nach dem Niedersächsischen Beamtengesetz (§ 101 NBG).“

FAQ 4.1: Wie komme ich mit personenbezogenen Daten in Berührung?

Personenbezogene Daten werden mir im Regelfall schriftlich, z. B. durch Verwaltungsvorlagen oder mündlich durch Erläuterungen und Diskussionen in Gremien, aber im Einzelfall auch telefonisch mitgeteilt, um über einen Sachverhalt entscheiden zu können.
Beinhalten zum Beispiel die Sitzungsunterlagen personenbezogene Daten (zum Beispiel bei Grundstücksangelegenheiten, im Zusammenhang mit Bewerbungen oder bei Vergabeentscheidungen), weil diese Daten für die Diskussion benötigt werden, so ist bereits ein Grundkonflikt vorprogrammiert. Dieser Konflikt besteht in der Wahrung des Persönlichkeitsschutzes einerseits und der Notwendigkeit, auf aussagekräftige Entscheidungsunterlagen zurückgreifen zu können, andererseits.

FAQ 4.2: Wie gelange ich an die für meine politische Arbeit notwendigen Informationen?

Die Verwaltung bereitet die Sitzungen durch die Aufstellung und öffentliche Bekanntmachung der Tagesordnung vor. Die Tagesordnung muss mir als Ratsmitglied zugeleitet werden. Die Form der Übersendung kann in der Geschäftsordnung des Rates geregelt werden und unter Berücksichtigung moderner Medien (z. B. per Fax, E-Mail oder über ein Ratsinformationssystem) erfolgen. Die Verwaltung hat darauf zu achten, dass der Versand der Unterlagen in einer Form erfolgt, die vor der Einsicht oder dem Zugriff Dritter geschützt ist (bei Papierversand sinnvollerweise: geschlossener Umschlag). Zudem ist es ratsam, den Umschlag mit einem Vertraulichkeitsvermerk zu kennzeichnen.

FAQ 4.3: Wer darf Kenntnis von personenbezogenen Daten erhalten?

Hier gilt zunächst als oberstes Prinzip der Grundsatz der Erforderlichkeit. Kenntnis von personenbezogenen Daten dürfen nur diejenigen Personen oder Gremien erlangen, die für die Bearbeitung und Entscheidungsfindung der jeweiligen Angelegenheit zuständig sind.

FAQ 4.4: Datenverarbeitung ist ein sehr komplexer Begriff. Was bedeutet er im Einzelnen?

Der Begriff Datenverarbeitung beinhaltet mehrere Komponenten, die in § 3 NDSG definiert sind. So ist

Erheben: das Beschaffen von Daten,
Speichern: das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger,
Verändern: das inhaltliche Umgestalten von Daten,
Übermitteln: das Bekanntgeben von Daten an Dritte,
Sperren: das Kennzeichnen von Daten, um ihre weitere Verarbeitung einzuschränken,
Löschen: das Unkenntlichmachen von Daten,
Nutzen: jede sonstige Verwendung von Daten.

FAQ 4.5: Was bedeutet das Datengeheimnis für meine politische Arbeit?

Das Datengeheimnis (§ 5 NDSG) verpflichtet mich, personenbezogene Daten, zu denen ich Zugang habe, nur zu dem Zweck zu verarbeiten, der für meine Aufgabenerfüllung vorgesehen ist. Gebe ich z. B. personenbezogene Daten, die ich von der Verwaltung erhalten habe, an meine Partei weiter, so verstoße ich gegen § 5 NDSG. Ich hätte damit eine Ordnungswidrigkeit nach § 29 Abs. 1 NDSG begangen, die mit einer Geldbuße bis zu 50.000 Euro geahndet werden kann (§ 29 Abs. 2 NDSG). Im Einzelfall könnte es sich sogar um eine Straftat nach § 28 Abs. 1 NDSG handeln.

FAQ 4.6: Was bedeutet Datensparsamkeit?

Datensparsamkeit ist ein essentieller Grundsatz im Datenschutzrecht. Es gilt die Devise „So wenig wie möglich, so viel wie nötig“, was die Datenmenge anbetrifft. Detailangaben sind oftmals nicht unbedingt erforderlich. So ist z. B.:

- die Benennung einer genauen Adresse mit Straße und Hausnummer manchmal nicht nötig. Die Auskunft über den Wohnort kann ausreichend sein,
- das genaue Geburtsdatum oftmals nicht erforderlich; die Angabe des Alters in Jahren kann reichen,
- der Familienstand (ledig, geschieden, getrennt lebend) nicht immer anzugeben. Die Angabe “nicht verheiratet“ kann genügen,
- bei Stellenbesetzungen die genaue Benennung von früheren und derzeitigen Arbeitgebern nicht vorzunehmen. Hier kann es ausreichen, die Art des Unternehmens oder die Branche anzugeben. Dies gilt insbesondere bei Bewerberinnen und Bewerbern in ungekündigter Stellung, die vielfach nicht wünschen, dass ihre Bewerbung dem derzeitigen Arbeitgeber bekannt wird.

FAQ 4.7: Im Zuge des Kommunalwahlkampfes möchte ich mir personenbezogene Daten der älteren Mitbürgerinnen und Mitbürger in meiner Kommune von der Verwaltung besorgen. Darf ich das?

„Die Meldebehörde darf Trägern von Wahlvorschlägen im Zusammenhang mit Parlaments- und Kommunalwahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über die in § 33 Abs. 1 bezeichneten Daten von nach dem Lebensalter bestimmten Gruppen von Wahlberechtigten erteilen." So lautet § 34 Abs. 1 Satz 1 des Niedersächsischen Meldegesetzes (NMG).

Hieraus folgt, dass grundsätzlich meine Partei oder Wählergruppe als Trägerin von Wahlvorschlägen berechtigt ist, die Daten anzufordern und zu Wahlwerbezwecken zu nutzen. Allerdings bestehen keine datenschutzrechtlichen Bedenken, wenn meine Partei/Wählergruppe mir die Daten der Personen übermittelt, die in meinem Wahlkreis wahlberechtigt sind. Deshalb bestehen auch keine Bedenken, wenn mir die Meldebehörde diese Daten direkt zur Verfügung stellt.

Die folgenden Daten sind in § 33 Abs. 1 NMG genannt und dürfen an meine Partei bzw. mich übermittelt werden:

- Vor- und Familiennamen,
- Doktorgrad und
- Anschriften.

Diese so genannte „Melderegisterauskunft in besonderen Fällen" bezieht sich auf klar umgrenzte Bevölkerungsgruppen eines bestimmten Lebensalters. Es ist also unzulässig, wenn ein Verzeichnis der Bürgerinnen und Bürger „zwischen 18 und 100 Jahren" angefordert wird, denn damit bekäme man eine Aufstellung aller wahlberechtigten Bürgerinnen und Bürger der Kommune. Fordert man hingegen eine Liste aller Seniorinnen und Senioren über 60 Jahren an, so ist dies zulässig, da es sich um eine begrenzte Gruppe von Personen handelt.

Die Betroffenen haben übrigens nach § 34 Abs. 5 NMG das Recht, einer Übermittlung ihrer Daten an Parteien und Wählergruppen zu widersprechen.

Meine Partei oder Wählergruppe muss die Daten im Übrigen spätestens einen Monat nach der Wahl löschen oder an die Meldebehörde zurückgeben. Gleiches gilt für mich, wenn ich Daten erhalten habe. Bitte nicht vergessen!

Eine Nutzung der Daten zu anderen Zwecken, z. B. zur Mitgliederwerbung, ist übrigens nicht zulässig.

FAQ 4.8: Kann ich außerhalb der Sechsmonatsfrist vor Wahlen gemäß § 33 Abs. 3 NMG mit Hilfe der so genannten „Gruppenauskunft" Daten aus dem Melderegister bekommen?

Nein! Eine Gruppenauskunft darf nur erteilt werden, wenn sie im öffentlichen Interesse liegt. Unter öffentlichem Interesse ist vor allem das Interesse der Allgemeinheit zu verstehen, das über das Individualinteresse einzelner Personen oder Gruppen weit hinausgeht. Deshalb sind Gruppenauskünfte außerhalb der „Wahlkampfzeit" selbst an Parteien und Wählergruppen in aller Regel unzulässig – umso mehr gilt dies für Auskünfte an mich als Einzelperson.

FAQ 4.9: Wie verhält es sich bei Jubiläen?

Als MT darf mir die Meldebehörde eine Auskunft über Alters- und Ehejubiläen des kommenden Monats erteilen. Die Auskunft darf nur

- Vor- und Familiennamen,
- Doktorgrad und
- Anschriften

sowie den Tag und die Art des Jubiläums umfassen.
Alters- und Ehejubiläen sind im NMG gesetzlich nicht definiert.

FAQ 4.10: Darf ich auch weitergehende Informationen über einzelne Personen einholen?

Die so genannte erweiterte Melderegisterauskunft gemäß § 33 Abs. 2 NMG ist nur an Personen, die ein berechtigtes Interesse glaubhaft machen können, zulässig. Die Rechtsprechung hat ein berechtigtes Interesse definiert als „ein nach vernünftiger Abwägung durch die Sachlage gerechtfertigtes Interesse, das rechtlicher, wirtschaftlicher oder ideeller Natur sein kann und das von der Rechtsordnung anerkannt ist." Ein berechtigtes Interesse ist also nahezu jedes Interesse außerhalb der reinen Neugier.
Wenn ich ein solches berechtigtes Interesse glaubhaft machen kann, darf mir die Meldebehörde zusätzlich zu Vor- und Familiennamen, Doktorgrad und Anschriften folgende Daten einer bestimmten Person mitteilen:

- Tag und Ort der Geburt,
- frühere Vor- und Familiennamen,
- Familienstand, beschränkt auf die Angaben, ob verheiratet oder nicht,
- Staatsangehörigkeiten,
- frühere Anschriften,
- Tag des Ein- und Auszugs,
- gesetzliche Vertreter sowie
- Sterbetag und -ort.

Allerdings muss ich mein berechtigtes Interesse bezogen auf jedes einzelne der vorstehenden Daten glaubhaft machen, sonst darf mir die Meldebehörde das Datum nicht mitteilen.
Die Meldebehörde hat die betroffene Person außerdem darüber zu informieren, dass sie mir eine erweiterte Melderegisterauskunft erteilt hat!

FAQ 4.11: Wie können behördliche Datenschutzbeauftragte bei Fragen des Datenschutzes helfen?

Behördliche Datenschutzbeauftragte unterstützen die öffentlichen Stellen bei der Sicherstellung des Datenschutzes und wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften hin. Für die Beauftragten gilt Weisungsfreiheit; sie können sich unmittelbar an die Behördenleitung wenden und dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden.
Jede öffentliche Stelle hat nach § 8a NDSG eine Beauftragte oder einen Beauftragten für den Datenschutz zu bestellen. Die Bestellung hat unabhängig von der Mitarbeiterzahl der öffentlichen Stelle zu erfolgen. Es ist aber möglich, dass z. B. mehrere kleinere Gemeinden eine gemeinsame Beauftragte bzw. einen gemeinsamen Beauftragten bestellen. Ebenso kann die Aufgabe der/des behördlichen Datenschutzbeauftragten auf eine kommunale Datenzentrale übertragen werden. Die behördlichen Datenschutzbeauftragten wirken auf die Einhaltung der datenschutzrechtlichen Vorschriften in ihrer Behörde hin. Sie haben zu prüfen, ob bei der Verarbeitung personenbezogener Daten die Grundsätze der Datenvermeidung und Datensparsamkeit eingehalten werden. Ferner obliegen ihnen u. a.

- die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme,
- die Prüfung, ob die technischen Maßnahmen nach dem jeweiligen Stand der Technik getroffen sind, um die datenschutzrechtlichen Vorschriften sicherzustellen,
- die Schulung der mit der Verarbeitung personenbezogener Daten befassten Mitarbeiterinnen und Mitarbeiter und
- die Beratung der Behördenleitung sowie einzelner Fachbereiche, Abteilungen und Ämter in Fragen des Datenschutzes und der Datensicherung.

Eine weitere wichtige Aufgabe der behördlichen Datenschutzbeauftragten besteht darin, dass sie auf der örtlichen Ebene eine datenschutzrechtliche Ombudsfunktion wahrnehmen. Das bedeutet, dass sich Bürgerinnen und Bürger, die sich durch die öffentliche Stelle in ihrem Recht auf informationelle Selbstbestimmung verletzt fühlen, direkt an die behördlichen Datenschutzbeauftragten wenden können. Dasselbe gilt für die Bediensteten der Behörde.

Als MT habe ich allerdings keinen direkten Auskunftsanspruch gegenüber behördlichen Datenschutzbeauftragten, sondern muss mich bei den für meine Mandatsausübung notwendigen Fragen des Datenschutzes grundsätzlich an die Bürgermeisterin oder den Bürgermeister (§ 39a NGO) wenden.

FAQ 4.12: Als Ratsmitglied darf ich bei allen Ausschusssitzungen anwesend sein, auch wenn ich dem Ausschuss nicht angehöre. Worin besteht in diesen Fällen mein Recht auf Information?

Das Recht, an allen Sitzungen der Ratsausschüsse, egal ob diese in öffentlicher oder nichtöffentlicher Sitzung tagen, zuhörend teilzunehmen, auch wenn ich diesen nicht angehöre, ergibt sich aus § 52 Abs. 2 NGO. Einen gesonderten Anspruch auf Informationen (insbesondere Beschlussvorlagen) für einzelne Ratsmitglieder, die dem Ausschuss nicht angehören, gibt es grundsätzlich nicht. Dieser Grundsatz wird nur dann außer Kraft gesetzt, wenn ein Ratsmitglied im Rat oder einem anderen Ausschuss einen Antrag gestellt hat und dieser Antrag nun in einem Ausschuss beraten werden soll, dem er nicht angehört. In diesem Sonderfall hat das Ratsmitglied alle Mitgliedschaftsrechte zu dem entsprechenden Tagesordnungspunkt bis auf das Recht, an der Abstimmung teilzunehmen.

FAQ 4.13: Haben stellvertretende Ausschussmitglieder dieselben Rechte auf Information wie die ordentlichen Ausschussmitglieder?

Im Verhinderungsfall übergibt das Ausschussmitglied die Sitzungsunterlagen üblicherweise an seine Vertreterin oder seinen Vertreter und erhält sie nach der Sitzung von diesen auch wieder zurück. Fällt ein Ausschussmitglied derartig kurzfristig aus, dass es die Sitzungsunterlagen persönlich nicht mehr rechtzeitig an seine Vertretung weitergeben kann, so kann sich die Vertreterin oder der Vertreter die Unterlagen bei ihrer/seiner Fraktion besorgen. Der Fraktion steht immer ein kompletter Satz der jeweiligen Sitzungsunterlagen zur Verfügung.

FAQ 4.14: Wie viele und welche Daten sind für die Entscheidungsfindung erforderlich?

Es kommt auf den Einzelfall an. So hat zum Beispiel das Verwaltungsgericht Oldenburg (Az. 2 VG D 33/83, nicht veröffentlicht) entschieden, dass die Beschlussorgane durch die Vorbereitung der Verwaltung (dies geschieht im Regelfall durch Beschlussvorlagen und in einfachen Fällen durch mündliche Erläuterungen in den Sitzungen) in die Lage versetzt

werden sollen, in Kenntnis aller für ihre Entscheidung relevanten tatsächlichen und rechtlichen Umstände zu beschließen. Es ist zum Beispiel anerkannt, dass bei Entscheidungen über Verträge regelmäßig die Vorlage der Vertragsentwürfe erforderlich ist. Ebenso muss bei einer Pensionierung aus gesundheitlichen Gründen dem zuständigen Gremium der Inhalt des ärztlichen Gutachtens vorliegen.

FAQ 4.15: Bei meiner Kommune liegen Stellenbewerbungen vor, über die ich als Mitglied des Verwaltungsausschusses zu entscheiden habe. Welche Informationen über die Bewerberinnen und Bewerber darf ich bekommen?

Bei der Vorstellung einer Stellenbewerberin oder eines Stellenbewerbers darf die Verwaltung nur die für die Entscheidungsfindung erforderlichen Daten/Unterlagen an das zuständige Gremium weiterleiten. Konkret bedeutet dies, dass die Weiterleitung von Informationen z. B. über soziale Kriterien (Angaben über Ehegatten und Familienangehörige, Anzahl der Kinder oder über den Bezug von Sozialleistungen) in der Regel unzulässig ist. Eine pauschale Eingrenzung der erforderlichen Datenmenge ist allerdings nicht möglich. So hat das Verwaltungsgericht Hannover (Beschluss vom 18.12.2000, Aktenzeichen 13 B 5619/00, Verwaltungsrechtsreport Nord (VwRR N) 2001, S. 50) beispielsweise entschieden, dass es grundsätzlich geboten ist, eine Übersicht über die Schul- und Berufsausbildung der Bewerberinnen und Bewerber sowie über ihren beruflichen Werdegang beizufügen. Zudem sollte, so das Gericht, bei Kandidatinnen und Kandidaten, die in die engere Wahl kommen, der wesentliche Inhalt zeitnaher dienstlicher Beurteilungen zusammengefasst vorgelegt werden.

Eine Änderung des Stellenplans kommt grundsätzlich ohne die Erhebung personenbezogener Daten aus. Lediglich der Vollzug, also die konkrete Besetzung der Stelle, erfordert die Weitergabe von Personaldaten an das zuständige Gremium.

FAQ 4.16: Um mit der örtlichen Presse sachgerecht über die anstehende Neufestsetzung der Gewerbesteuerhebesätze diskutieren zu können, erbitte ich mir eine betriebsbezogene Aufstellung, aus der ich ersehen kann, welche Gewerbebetriebe in welcher Höhe Gewerbesteuer zahlen. Darf mir die Bürgermeisterin/der Bürgermeister diese Aufstellung zuleiten?

Die Bürgermeisterin oder der Bürgermeister darf mir diese Aufstellung nicht zuleiten! In der Abgabenordnung (AO) wird das Steuergeheimnis besonders geschützt (§ 30 AO). Danach ist die Weitergabe der Daten im vorliegenden Fall nur dann möglich, wenn diese Daten für ein Verwaltungsverfahren benötigt werden. Allenfalls könnten anonymisierte Daten, so z. B. Zahlen über das Gesamtaufkommen an Gewerbesteuer der letzten Jahre, weitergegeben werden.

FAQ 4.17: Ich möchte im Rat einen Antrag stellen, dass sozial bedürftige Personen künftig geringere Eintrittsgelder für die städtischen Schwimmbäder zahlen. Um diesen Personenkreis gezielt über meinen Antrag informieren zu können, erbitte ich mir eine Adressliste der Sozialhilfeempfänger/innen in unserer Stadt. Darf mir die Bürgermeisterin/der Bürgermeister diese Liste aushändigen ?

Nein! Die Daten dürfen nur mit Einverständnis der Betroffenen weitergegeben werden, da die Daten nicht zu dem Zweck verwendet werden sollen, für den sie erhoben wurden (Grundsatz der Zweckbindung). Zudem ist auch kein gesetzlicher Grund für die Datenweitergabe gegeben (§ 35 des SGB I in Verbindung mit § 67b SGB X). Das Ziel, die Be-

troffenen zu informieren, kann ich über die örtliche Presse, einen Wahlkampfstand oder Flugblätter erreichen.

FAQ 4.18: Darf ich während einer Ratssitzung fotografieren?

Grundsätzlich dürfen während einer öffentlichen Gemeinderatssitzung Fotografien angefertigt werden. Voraussetzung ist, dass die Fotos offen und für jedermann erkennbar gemacht werden, die Fotografierten keine Einwände dagegen haben und die Fotos nur mit dem Einverständnis der fotografierten Personen weiter verwendet werden. Der ordnungsgemäße Ablauf der Sitzung darf zudem nicht gestört werden .

FAQ 4.19: Sind Tonbandaufzeichnungen des Protokollführers während der Ratssitzung erlaubt?

Die Verwendung von Tonbändern zur ordnungsgemäßen Erstellung der Niederschrift ist nicht unumstritten. Dennoch geht die herrschende Rechtsauffassung davon aus, dass Tonbandaufzeichnungen als Hilfsmittel zur Erstellung der Niederschrift zulässig sind, insbesondere wenn der Rat dies in seiner Geschäftsordnung ausdrücklich bestimmt hat (vgl. Kommentierung Thiele zu § 49 NGO). Wichtig ist in diesem Zusammenhang, dass die Tonbandaufzeichnung nach der Genehmigung der Niederschrift durch den Rat von der Verwaltung gelöscht wird. Bis zur Genehmigung der Niederschrift kann jedes Ratsmitglied die Tonbandaufzeichnungen abhören.

FAQ 4.20: Wie ist mit Sitzungsniederschriften zu verfahren?

Gegen die Veröffentlichung von Verlaufs-/Ergebnisprotokollen über öffentliche Sitzungen bestehen aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken. Wortprotokolle und Protokolle, die schützenswerte personenbezogene Daten beinhalten, sollten nur den tatsächlichen Sitzungsteilnehmerinnen und -teilnehmern bzw. in einem Exemplar den Fraktionen zugeleitet werden. Niederschriften nichtöffentlicher Sitzungen sind nur denjenigen Ratsmitgliedern zuzusenden, die an der Sitzung teilgenommen haben.

FAQ 4.21: Darf ich Sitzungsunterlagen weitergeben?

Nein! Das Weitergabeverbot von Unterlagen mit personenbezogenen Daten bezieht die Mitteilung des Inhaltes an Dritte mit ein. Dies gilt für mündliche und schriftliche Mitteilungen. Als Dritte einzustufen sind hier nicht nur Familienmitglieder, Kollegen, Bekannte, Nachbarn etc., sondern auch Parteifreunde. Endet mein Mandat, so muss ich alle verbliebenen Unterlagen an die Verwaltung zurückgeben bzw. datenschutzgerecht vernichten.
Generell bin ich als MT verpflichtet, alle erhaltenen Unterlagen mit personenbezogenen Daten gegen die Kenntnisnahme oder den Zugriff Dritter zu sichern. Sitzungsunterlagen sind keine privaten Unterlagen, sondern ausschließlich für den Verwaltungsgebrauch bzw. meine Arbeit als MT bestimmt.

FAQ 4.22: Ein Journalist erbittet von mir Informationen über eine nichtöffentliche Sitzung des Verwaltungsausschusses. Er verweist mich darauf, dass nach dem Niedersächsischen Pressegesetz eine Auskunftsverpflichtung der Gemeinde besteht. Wie verhalte ich mich?

Ich bin als MT grundsätzlich nicht verpflichtet, dem Journalisten Auskünfte zu erteilen. Die grundsätzliche Auskunftsverpflichtung der Gemeinde hingegen gegenüber der Presse ergibt sich aus § 4 des Niedersächsischen Pressegesetzes. Danach sind die Behörden ver-

pflichtet, den Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. Ich kann den Journalisten an die Bürgermeisterin/den Bürgermeister verweisen, da dieser/diesem die Unterrichtung der Presse über Angelegenheiten der Gemeinde im Rahmen der Unterrichtungspflicht der Bevölkerung obliegt (§ 62 Abs. 3 NGO), und sie/er prüfen muss, ob es Gründe gibt, die Auskunft zu verweigern. Dies kann zum Beispiel gegeben sein, wenn mit der Erteilung der Auskunft ein überwiegendes öffentliches oder ein schutzwürdiges privates Interesse verletzt würde.

FAQ 4.23: Darf ich Notizen aus einer Gemeinderatssitzung veröffentlichen, z. B. im Internet?

Zu öffentlichen Sitzungen des Gemeinderates hat grundsätzlich jedermann Zutritt. Den Zuhörern ist es gestattet, sich Notizen zu machen und daraus einen aus dem Gedächtnis verfassten Bericht z. B. im Internet zu veröffentlichen. Das gilt auch für mich als MT, sofern sich meine Veröffentlichung auf diejenigen Vorgänge beschränkt, die in der öffentlichen Sitzung zur Sprache gekommen sind. Bei meiner Publikation muss jedoch klar erkennbar sein, dass es sich um persönliche Aufzeichnungen handelt und nicht um eine Veröffentlichung der Gemeinde oder eine amtliche Niederschrift.

FAQ 4.24: Was passiert mit personenbezogenen Daten, wenn ich sie für meine Mandatstätigkeit nicht mehr benötige, weil der Vorgang abgeschlossen ist?

Personenbezogene Daten sind unverzüglich zu löschen, bzw. zu vernichten, wenn sie nicht mehr erforderlich sind. Meine Arbeit als MT wird durch die Datenvernichtung nicht beeinträchtigt, weil ich als Gremienmitglied bei Bedarf jederzeit im Rahmen meiner Zuständigkeiten auf die archivierten Dokumente bei der Verwaltung oder meiner Fraktion zurückgreifen kann.

FAQ 4.25: Gibt es Mindestanforderungen für die Vernichtung von Unterlagen?

Dokumente, die personenbezogene Daten enthalten, dürfen keinesfalls über den Hausmüll oder die Altpapierabholung entsorgt werden. Auch das Zerreißen oder das einfache „In-Streifen-Schneiden“ (Schreddern) von Papierseiten ist meist nicht ausreichend.
Gleiches gilt für elektronische Datenträger in Form von Disketten, CDs, DVDs oder (Wechsel-)festplatten. Die Löschung der Daten muss dergestalt erfolgen, dass eine spätere Wiederherstellung der Daten ausgeschlossen ist.

FAQ 4.26: Dürfen Daten von Rats- und/oder Ausschussmitgliedern durch die Verwaltung bekannt gegeben werden?

Veröffentlicht eine Kommune in ihren Publikationsorganen die Zusammensetzung der Gremien mit näheren Angaben zu den Mitgliedern, so ist dagegen nichts einzuwenden, wenn sich die Angaben auf diejenigen persönlichen Daten beschränken, die anlässlich der Kommunalwahl öffentlich bekannt gemacht worden sind.

FAQ 4.27: Darf ich als MT in die über mich gespeicherten Daten bei der Verwaltung Einsicht nehmen ?

§ 16 NDSG regelt die Rechte der Betroffenen. Die Daten verarbeitende Stelle muss mir auf Antrag Auskünfte erteilen über die zu meiner Person gespeicherten Daten. Auch der Zweck und die Rechtsgrundlage der Speicherung sowie die Herkunft der Daten und die Empfänger von eventuellen Übermittlungen müssen mir bekannt gegeben werden. Die-

ser Auskunftsanspruch ist ein wesentlicher Bestandteil meines Rechts auf informationelle Selbstbestimmung und gilt selbstverständlich für alle Bürgerinnen und Bürger, unabhängig von Alter, Nationalität, Wohnsitz oder Geschlecht.
Der Antrag auf Auskunft ist form- und fristlos, sinnvollerweise aber schriftlich zu stellen. Die Auskunft und die Akteneinsicht sind kostenlos.

FAQ 4.28: Kann mir die Auskunft verweigert werden?

Die Auskunft kann verweigert werden, wenn die Auskunftserteilung den ordnungsgemäßen Arbeitsablauf der Daten verarbeitenden Stelle beeinträchtigt. Des Weiteren darf die öffentliche Sicherheit nicht gefährdet werden, und dem Bund und den Ländern dürfen keine Nachteile entstehen. Ein dritter Hinderungsgrund der Auskunftserteilung besteht darin, dass die personenbezogenen Daten auf Grund einer Rechtsvorschrift oder wegen berechtigter Interessen Dritter geheim zu halten sind (§ 16 Abs. 4 NDSG).

FAQ 4.29: Kann ich die Verarbeitung meiner personenbezogenen Daten verhindern?

§ 17a NDSG sieht ein Widerspruchsrecht für Betroffene vor. Wenn also schutzwürdige persönliche Gründe vorliegen, kann ich der Daten verarbeitenden Stelle gegenüber Widerspruch gegen die Verarbeitung meiner Daten einlegen. Überwiegen meine persönlichen Gründe das Interesse der öffentlichen Stelle an der Datenverarbeitung, so ist die Verarbeitung unzulässig.
Das Widerspruchsrecht gilt nicht, wenn eine Rechtsvorschrift die Datenverarbeitung verpflichtend vorsieht.

FAQ 4.30: Wie werden Verstöße gegen das Datenschutzrecht geahndet?

Wer personenbezogene Daten, die nicht allgemein zugänglich sind, entgegen der Zweckbindung (§ 5 NDSG) verarbeitet, offenbart, sich durch Vortäuschung falscher Tatsachen verschafft oder an sich oder andere übermitteln lässt, handelt ordnungswidrig. Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 Euro belegt werden (§ 29 NDSG).
Strafbar macht sich sogar, „wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, personenbezogene Daten, die nicht allgemein zugänglich sind,

1. unbefugt erhebt, speichert, verändert, löscht, übermittelt oder nutzt oder
2. durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst."

Auch der Versuch ist strafbar. Ein Verstoß wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe geahndet (§ 28 NDSG).

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.
(4) Das Nähere bestimmt ein Gesetz. Dieses Gesetz kann personalrechtliche Entscheidungen, welche die der Landesbeauftragten oder dem Landesbeauftragten für den Datenschutz zugeordneten Bediensteten betreffen, von deren oder dessen Mitwirkung abhängig machen. Das Gesetz kann weitere Aufgaben der Landesbeauftragten oder des Landesbeauftragten für den Datenschutz vorsehen.

Der Landesbeauftragte für den Datenschutz Niedersachsen