daten
schutz

XVII. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2003 – 2004

Herausgeber: Der Landesbeauftragte für den Datenschutz Niedersachsen
~~Brühlstraße 9, 30169 Hannover~~ Prinzenstraße 5, 30159 Hannover
Postfach 221, 30002 Hannover

Verantwortlich: Burckhard Nedden

Layout: set-up design.print.media
An der Markuskirche 1 · 30163 Hannover

Druck: Landesvermessung und Geobasisinformation Niedersachsen
Podbielskistraße 331 · 30659 Hannover

Hannover, den 15.11.2004

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

XVII. Tätigkeitsbericht

des Landesbeauftragten
für den Datenschutz Niedersachsen
für die Jahre 2003 – 2004

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.

Vorwort und Einführung

Hiermit lege ich den XVII. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 2003 und 2004 vor. Redaktionsschluss war der 15. November 2004.

Das veränderte Format und die verbesserte graphische Gestaltung sind Ausdruck eines ganz neuen Ansatzes: Der Tätigkeitsbericht will nach dem Beispiel anderer Jahresberichte in Wirtschaft und Verwaltung in der Art einer Management summary in stark komprimierter Form über wichtige Entwicklungen des Datenschutzes und über bedeutsame Ergebnisse meiner Arbeit informieren und den sich daraus für die Zukunft ergebenden Handlungsbedarf darstellen. Nicht mehr die ausführliche und detailreiche Schilderung von Einzelfällen soll im Vordergrund stehen, sondern es sollen die übergreifenden datenschutzrechtlichen und datenschutzpolitischen Entwicklungslinien aufgezeigt werden. Auf diese Weise soll eine noch bessere Grundlage für eine problembezogene Erörterung des Tätigkeitsberichts insbesondere im Landtag und in seinen Ausschüssen erreicht werden. Die Erfahrungen der vergangenen Jahre belegen überdeutlich, dass die bisher dem Parlament vorgelegten, sehr umfangreichen und ins Detail gehenden Tätigkeitsberichte mit ihrer Überfülle an Material eine solche Erörterung wohl eher behindert haben. Die fundierte Dokumentation der Einzelergebnisse meiner Tätigkeit geht dabei aber nicht verloren; sie findet sich themenbezogen zusammen mit den daraus abzuleitenden Handlungsempfehlungen für die Datenschutzpraxis in Behörden und Betrieben in meinem Internetangebot (www.lfd.niedersachsen.de). Das Internetangebot wird auf diese Weise zunehmend auch die Funktion einer kontinuierlichen und aktuellen Berichterstattung über unsere Aktivitäten übernehmen.

Der Arbeitsaufwand für die Erstellung des Tätigkeitsberichts und für die nach § 22 Abs. 3 Satz 2 NDSG ebenfalls dem Landtag vorzulegende Stellungnahme der Landesregierung lässt sich mit diesem neuen Ansatz ganz wesentlich reduzieren. Mehrkosten für Gestaltung und Druck des Tätigkeitsberichtes sind im Ergebnis nicht entstanden, weil der Aufwand, der bisher für Erstellung und Druck des Tätigkeitsberichts als Landtags-Drucksache entstanden war, entfallen ist.

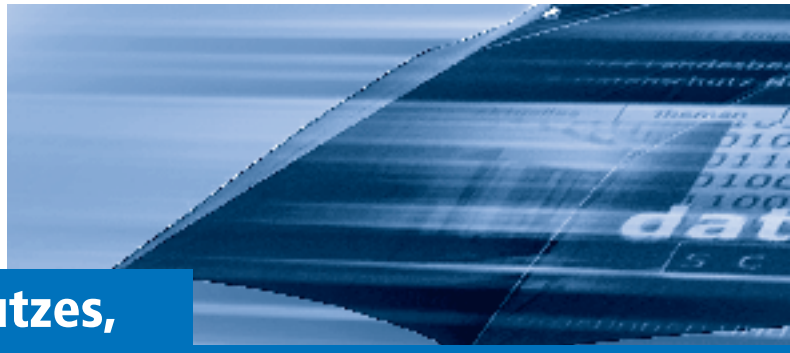
Ich hoffe sehr, dass die Informationswirkung des Tätigkeitsberichtes, insbesondere gegenüber dem Parlament und den Entscheidungsträgern in Verwaltung und Wirtschaft, durch den neuen Ansatz weiter verbessert wird und dass dadurch zugleich die Sensibilität für eine angemessene Berücksichtigung datenschutzrechtlicher Anforderungen erhöht werden kann.

Meinen Mitarbeiterinnen und Mitarbeitern danke ich für ihre engagierte Arbeit, bei der immer deutlich geworden ist, dass die Belange des Datenschutzes nicht absolut gesetzt, sondern in ihrer Konkurrenz zu anderen Rechten oder rechtlich geschützten Interessen angemessen und sachgerecht eingeordnet werden.

Hannover, im November 2004

Burckhard Nedden
Landesbeauftragter für den Datenschutz

Inhalt

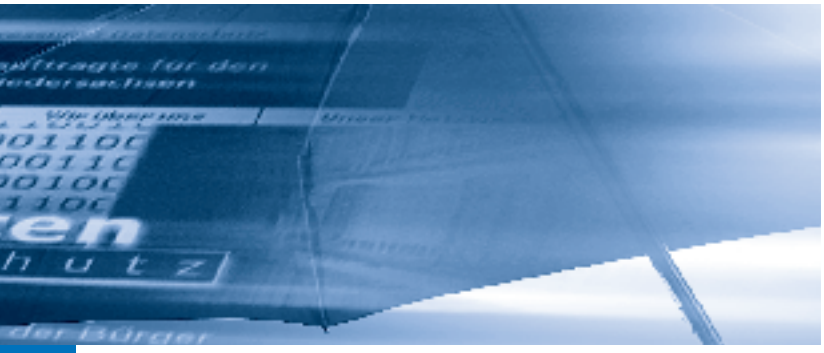


Die Situation des Datenschutzes, datenschutzrechtlicher Handlungsbedarf

Problemfelder

Die Diskussionen über die Einführung neuer Eingriffsinstrumente der Sicherheitsbehörden und über den Stellenwert von Datenschutz und informationeller Selbstbestimmung im Verhältnis zu der Verpflichtung des Staates, kollektive und individuelle Sicherheit zu gewährleisten, haben auch in den Jahren 2003 und 2004 die Arbeit der Datenschutzbeauftragten in Bund und Ländern weiterhin nachhaltig bestimmt. In Niedersachsen ist diese Diskussion insbesondere im Zusammenhang mit der Novellierung des Polizeirechts geführt worden (vgl. dazu unter Nr. 2). Ich hatte Gelegenheit, meine Argumente in einer Anhörung des für die Beratung federführenden Landtagsausschusses vorzutragen; dabei habe ich allerdings nicht den Eindruck gewonnen, bei der Ausschussmehrheit noch auf eine offene Entscheidungssituation zu treffen. Dies liegt ganz offensichtlich an dem für das deutsche parlamentarische System mittlerweile überall kennzeichnenden Zusammenwirken der jeweiligen Mehrheitsfraktion(en) mit der von ihr (ihnen) getragenen Regierung: Entscheidende Weichenstellungen und die Bewertung von möglichen Konfliktfeldern, z. B. solchen aus Sicht des Datenschutzes, werden dabei zumeist weit im Vorfeld der parlamentarischen Beratungen vorgenommen, so dass etwaige Stellungnahmen im Rahmen des förmlichen parlamentarischen Verfahrens einfach zu spät kommen. Diese Entwicklung macht es generell schwer, die gesetzlich vorgesehene Beratungsfunktion des Landesbeauftragten für den Datenschutz gerade auch gegenüber dem Landtag (§ 22 Abs. 1 Satz 3 NDSG) effektiv auszuüben.

Umso wichtiger ist es, dass ich – so wie im Gesetz auch vorgegeben (§ 22 Abs. 1 Satz 4 NDSG) – von der Landesregierung und den Ressorts frühzeitig bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften mit datenschutzrechtlicher Bedeutung beteiligt werde. Hier ergab sich – leider – mehrfach die Notwendigkeit, Ressortleitungen an die Einhaltung dieser gesetzlichen Vorgabe erinnern zu müssen. Gerade bei dem für das Datenschutzrecht zuständigen Ministerium ist die Zusammenarbeit insofern noch deutlich verbesserungsbedürftig. Auch bei Anfragen des LfD und bei erbetenen Stellungnahmen waren die Reaktion dieses Ministeriums häufiger sehr zögerlich. Die unbestreitbaren Zielkonflikte zwischen dem Auftrag des Ministeriums zur Gewährleistung der öffentlichen Sicherheit einerseits und Datenschutz und informationeller Selbstbestimmung andererseits dürfen nicht als Hindernis für eine rechtzeitige Information und einen offenen Meinungsaustausch herangezogen werden, zumal ich und alle meine Mitarbeiterinnen und Mitarbeiter bei der Vertretung datenschutzrechtlicher Belange immer das gebotene Augenmaß eingehalten und keine überzogenen Positionen vertreten haben.



Kooperation und Beratung als Kernfunktionen und Dienstleistung

Im übrigen hat sich die Zusammenarbeit mit den Ressorts weiter gut entwickelt. Unsere datenschutzfachliche Beratungskompetenz im Vorfeld von rechtlichen, organisatorischen oder technischen Lösungen wird rege in Anspruch genommen und häufig durch unmittelbare Einbindung in Projekt- oder Arbeitsgruppen realisiert. Mit den Datenschutzbeauftragten der Hochschulen, der Landeskrankenhäuser und der Justizvollzugsanstalten sind neue Netzwerke geknüpft oder die bestehenden Arbeitskontakte verstärkt worden. Besonders hervorzuheben ist die sehr gute Zusammenarbeit mit den Kommunalen Spitzenverbänden in allen Fragen des eGovernment.

Die Zusammenarbeit im nichtöffentlichen Bereich mit den Unternehmen, Verbänden und Organisationen der Wirtschaft hat sich sehr erfreulich entwickelt. Es ist überall mit großer Zustimmung aufgenommen worden, dass es in der Datenschutzaufsicht eine Neuausrichtung der Handlungsansätze und der Prüfstrategie gegeben hat und dass nicht mehr die nachsorgende Kontrolle und die Aufdeckung von Datenschutzverstößen im Vordergrund unserer Arbeit stehen, sondern die vorsorgende konstruktive Beratung und Mitgestaltung bei der Entwicklung von datenschutzgerechten Lösungen im Sinne einer aktiven Dienstleistung. Der Sachverstand und die Beratungskompetenz meiner Mitarbeiterinnen und Mitarbeiter wird mittlerweile in erfreulichem Umfang von den Unternehmen nachgefragt. Die gemeinsam mit großen niedersächsischen Unternehmen und Verbänden erarbeitete Handreichung für einen datenschutzgerechten Internetauftritt der Wirtschaft oder die mit dem Niedersächsischen Einzelhandelsverband abgestimmten Hinweise zum Umgang mit Kundendaten (vgl. dazu unter Nr. 12) sind aktuelle Belege für diese gut entwickelte Zusammenarbeit zwischen Datenschutzaufsicht und Wirtschaft.

An solchen Beispielen wird auch deutlich, dass die seit 1992 bestehende Zusammenführung der Aufsichtsaufgaben für den öffentlichen und für den nichtöffentlichen Bereich beim Landesbeauftragten für den Datenschutz überaus sinnvoll ist und in erheblichem Umfang Synergien bei der Nutzung des rechtlichen und technischen Fachverstandes ermöglicht.

Eine ganz wichtige Rolle bei dem Ansatz, vorsorgend durch Beratung und Aufklärung datenschutzgerechte Lösungen mitzugestalten, spielt das im letzten Jahr in den Räumen meiner Geschäftsstelle eingerichtete Datenschutzinstitut Niedersachsen (DiN) mit seinen ständig erweiterten Fortbildungs- und Qualifizierungsangeboten im Bereich Datenschutz und Datensicherheit.

Datenschutzrechtliche Fortschritte

Der langjährige Dissens in der Frage, ob für die Videoüberwachung durch öffentliche Stellen eine eigenständige Regelung im NDSG erforderlich ist, ist mittlerweile beigelegt. Im Einvernehmen mit dem Innenministerium ist im NDSG ein neuer § 25a formuliert worden, der sich zurzeit in der parlamentarischen Beratung befindet und nun hoffentlich auch zügig verabschiedet wird. Die neue Regelung wird für mögliche Anwender insbesondere im kommunalen Bereich die rechtlichen Voraussetzungen einer Videoüberwachung eindeutig klarstellen und damit auch ein Stück Rechtssicherheit schaffen.

Die gemeinsam mit dem Sozialministerium aufgenommenen Arbeiten an einem Niedersächsischen Gesundheitsdatenschutzgesetz sind von allen Seiten mit großem Engagement weitergeführt worden. Es sind jedoch noch eine Vielzahl von Detailfragen zu klären, die in Teilen auch grundsätzliche Bedeutung haben. Daher werden die Arbeiten auch nicht kurzfristig abgeschlossen werden können. Die Arbeiten an dem Gesetzestext haben aber schon jetzt in vielen wichtigen Fragen des Gesundheitsdatenschutzes zu übereinstimmenden Auffassungen geführt, die bei der täglichen Arbeit zu Grunde gelegt werden können.

Einen großen Fortschritt hat es auch in der Zusammenarbeit mit der Steuerverwaltung gegeben. Nachdem die Meinungsverschiedenheiten über den Umfang der Kontrollbefugnisse des LfD in einem längeren, intensiven Diskussionsprozess ausgeräumt werden konnten, haben in der zweiten Jahreshälfte 2004 bei drei Finanzämtern die geplanten Beratungsbesuche stattgefunden. Bei diesen Besuchen sind unter Beteiligung der Oberfinanzdirektion als Aufsichtsbehörde Datenschutzfragen aus der Praxis des Besteuerungsverfahrens erörtert sowie gemeinsam Handlungsempfehlungen zur Sicherung von Betroffenenrechten und zum technisch-organisatorischen Datenschutz entwickelt worden. Die Beratungsbesuche werden im nächsten Jahr bei weiteren Finanzämtern fortgesetzt. Außerdem wird gemeinsam mit der Oberfinanzdirektion ein Konzept zur Einbeziehung des Themas Datenschutz in die Aus- und Fortbildungsaktivitäten der Steuerverwaltung erarbeitet.

Datenschutzrechtlicher Handlungsbedarf

Datenschutzrechtlichen Handlungsbedarf sehe ich für die nächste Zeit vor allem in den folgenden Bereichen:

- Die Vorgaben aus dem so genannten Lauschangriff-Urteil des Bundesverfassungsgerichts müssen in das Landesrecht übernommen werden. Dazu müssen eine Vielzahl von Einzelregelungen in den Sicherheitsgesetzen überprüft werden (vgl. dazu unter Nr. 1).
- Nach der Entscheidung des Bundesverfassungsgerichts über die Verfassungsbeschwerde eines niedersächsischen Bürgers gegen die Regelungen zur präventiven Telekommunikationsüberwachung im novellierten Polizeigesetz wird über die notwenigen Änderungen im § 33a Nds. SOG zu entscheiden sein (vgl. dazu unter Nr. 2).
- Die Landesregierung sollte bei Initiativen zur Ausdehnung der DNA-Analyse Augenmaß bewahren und sie danach beurteilen, ob die aus dem GG hergeleiteten Anforderungen des Bundesverfassungsgerichts eingehalten werden. Dazu gehört auch die Aufrechterhaltung angemessener Kontrollmechanismen (Richtervorbehalt) (vgl. dazu unter Nr. 3).
- Bei Regelungen zur Vergabe von Ordnungsnummern mit Personenbezug ist auf eine strikte Zweckbindung und auf klare Verwendungsverbote zu achten (vgl. dazu unter Nr. 4).
- Bei der Pilotierung und nachfolgenden Einführung des landeseinheitlichen Personalmanagementverfahrens (PMV) müssen die datenschutzrechtlichen Vorgaben zur Gewährleistung von Vertraulichkeit, Integrität und Authentizität der verarbeiteten Personaldaten sowie die nach der Vorabkontrolle erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit verlässlich umgesetzt werden (vgl. dazu unter Nr. 5). Entsprechendes gilt für die neuen automationsgestützten Verfahren zur Haushaltsbewirtschaftung (vgl. dazu unter Nr. 6).
- Bei der Aktion „Datenschutz in der Arztpraxis“ erhoffe ich mir die weitere Unterstützung des Sozialministeriums auch bei der für das nächste Jahr geplanten Ausweitung auf den Bereich der Krankenhäuser (vgl. dazu unter Nr. 9).
- Alle öffentlichen und privaten Stellen sollten beim Einsatz von Scoring-Verfahren deren datenschutzrechtliche Problematik im Auge behalten und insbesondere auf die Sicherung der Betroffenenrechte Bedacht nehmen (vgl. dazu unter Nr. 13).
- In den Behörden und Unternehmen müssen die bestehenden Funknetzwerke einer Risikoabschätzung unterzogen und die danach erforderlichen technisch-organisatorischen Absicherungsmaßnahmen gegen Angriffe und Missbrauch umgesetzt werden (vgl. dazu unter Nr. 16).
- Die Nds. Landesregierung sollte den eingeschlagenen Weg des eGovernment mit Nachdruck fortsetzen und dabei meine Handlungsempfehlungen für datenschutzgerechte Lösungen konsequent umsetzen (vgl. dazu unter Nr. 17).
- Nachdem nunmehr der Bund kurzfristig den Entwurf eines Informationszugangsgesetzes vorlegen wird, sollten die Landesregierung und die Politik ihren Widerstand gegen die Schaffung einer vergleichbaren niedersächsischen Regelung aufgeben (vgl. dazu unter Nr. 18).

Lauscher an der Wand 1

oder: Die Entscheidungen des Bundesverfassungsgerichts vom 03.03.2004 und ihre Folgen

Am 3. März 2004 hat des Bundesverfassungsgericht zwei Entscheidungen getroffen, die Politik, Sicherheitsbehörden und Datenschützer noch für lange Zeit beschäftigen werden.

Der so genannte Große Lauschangriff

In der ersten Entscheidung hatte der Erste Senat des Gerichts über die Verfassungsmäßigkeit der im Jahre 1998 vorgenommenen Änderung des Art. 13 Abs. 3 GG zu entscheiden. Das Gericht kommt zu dem Ergebnis, dass die vorgenommene Verfassungsänderung nicht verfassungswidrig ist. Art. 13 Abs. 3 GG sei mit Art. 79 Abs. 3 GG vereinbar. Demgegenüber sei jedoch ein erheblicher Teil der Vorschriften der Strafprozessordnung (StPO) zur Durchführung der akustischen Überwachung von Wohnraum zu Zwecken der Strafverfolgung (des sog. Großen Lauschangriffs) verfassungswidrig. Der Gesetzgeber sei verpflichtet, einen verfassungsgemäßen Rechtszustand bis spätestens zum 30. Juni 2005 herzustellen. Bis zu diesem Termin könnten die beanstandeten Normen nach Maßgabe der Gründe allerdings weiterhin angewandt werden, wenn gesichert ist, dass bei der Durchführung der Überwachung der Schutz der Menschenwürde gewahrt und der Grundsatz der Verhältnismäßigkeit eingehalten wird.

In den Gründen dieses Urteils hat das Bundesverfassungsgericht aus der in Art. 1 Abs. 1 GG geschützten Menschenwürde einen unantastbaren Kernbereich privater Lebensgestaltung abgeleitet, der jedem staatlichen Zugriff entzogen ist. Das Bundesverfassungsgericht unterstreicht die Absolutheit dieser Schranke mit folgenden Sätzen:

„Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen. Zwar wird es stets Formen von besonders gravierender Kriminalität und entsprechender Verdachtssituationen geben, die die Effektivität der Strafrechtspflege als Gemeinwohlinteresse manchem gewichtiger erscheinen lässt als die Wahrung der menschlichen Würde des Beschuldigten. Eine solche Wertung ist dem Staat jedoch durch Art. 1 Abs. 1, Art. 79 Abs. 3 GG verwehrt."

Das Gericht hat sich in dem Urteil zwar mit strafprozessualen, also repressiven Überwachungsmaßnahmen gemäß §§ 100a ff. StPO und den sich dafür aus dem Grundrecht des Artikels 13 i. V. m. Art. 1 Abs. 1 GG ergebenden Grenzen befasst, es hat aber die dort und die in seinem Urteil vom 14. Juli 1999 (BVerfGE 100, 313) entwickelten Grundsätze in seinem am gleichen Tag verkündeten

Beschluss zur (präventiven) Überwachung der Telekommunikation durch das Zollkriminalamt

auch im Bereich der Prävention dem Gesetzgeber zur Beachtung verbindlich vorgegeben, und zwar auch soweit eine Überwachung außerhalb von Wohnungen geschieht. Dabei wird sicherlich zu berücksichtigen sein, dass das Recht auf unbeobachtete Kommunikation dann in ganz besonderer Weise zu sichern ist, wenn die fragliche Kommunikation in dem durch Art. 13 GG geschützten Bereich stattfindet. Das Bundesverfassungsgericht hat jedoch unabhängig davon den besonderen Stellenwert dieses auch durch Art. 10 GG geschützten Rechts immer wieder betont und auch im Beschluss vom 3. März 2004 erneut hervorgehoben:

„Das Grundrecht aus Art. 10 Abs. 1 GG gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen (vgl. BVerfGE 67, 157, 171). Durch die Kenntnisnahme des Inhalts von Briefen und das Abhören von Telefongesprächen wird auf intensive Weise in das Grundrecht eingegriffen. Die Schwere des Eingriffs wird auch dadurch geprägt, dass der Betroffene wegen der gebotenen Heimlichkeit nicht an dem Anordnungsverfahren beteiligt ist."

Schutz des Kernbereichs auch außerhalb von Wohnungen

Durch diese Ausführungen des Bundesverfassungsgerichts, insbesondere auch durch den ausdrücklichen Verweis auf die Würde des Menschen als einzubeziehendem Schutzgut, wird klargestellt, dass auch bei Eingriffen in das Recht auf unbeobachtete Kommunikation, die außerhalb von Wohnungen stattfinden, der Kernbereich privater Lebensgestaltung von staatlicher Überwachung frei bleiben muss. Denn, wie das Bundesverfassungsgericht im Lauschangriff-Urteil im Leitzsatz 2 festgelegt hat, gehört „zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG (…) die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung".

Diese Grenze gilt auch über den besonderen Schutzbereich der Artikel 10 und 13 GG hinaus in allen Fällen, in denen durch öffentliche Stellen mit Hilfe einer verdeckten Datenerhebung in das Recht auf informationelle Selbstbestimmung eingegriffen wird; denn dieses Recht hat das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG und aus dem Schutz der Menschenwürde in

Art. 1 Abs. 1 GG hergeleitet. Auch bei Eingriffen in das Recht auf informationelle Selbstbestimmung bildet daher der Kernbereich privater Lebensgestaltung wegen seines engen Bezuges zu der durch Art. 1 Abs. 1 GG geschützten Menschenwürde eine absolute Schranke, die auch nicht durch Abwägung mit Straftatenverfolgungs-, Straftatenvorbeugungs- oder Gefahrenabwehrinteressen nach Maßgabe des Verhältnismäßigkeitsgrundsatzes relativiert werden darf.

Auswirkungen auf das niedersächsische Landesrecht

Danach müssen alle Regelungen im niedersächsischen Landesrecht, die durch verdeckte Datenerhebungen in das Recht auf unbeobachtete Kommunikation aus Artikel 10 und 13 GG oder in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG eingreifen, darauf hin überprüft werden, ob sie die Grenzen, die sich aus dem absolut geschützten Kernbereich privater Lebensgestaltung ergeben, sowie weitere, in den beiden Entscheidungen des Bundesverfassungsgerichts entwickelte Grundsätze, insbesondere auch verfahrensrechtlicher Art, einhalten.
Diese Überprüfung muss sich insbesondere auf die folgenden Bereiche beziehen:

Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG)

- Sicherstellung des absolut geschützten Kernbereichs privater Lebensgestaltung in den §§ 33a, 33b, 34, 35, 36 und 36a,
- Schutz von Gesprächen zwischen dem Überwachten und Personen nach § 53 StPO und von Gesprächen im engsten Familien- und Vertrautenkreis (§ 30 Abs. 6 Nds. SOG),
- Verwertungsverbot bei unvermeidlichen Eingriffen in den Kernbereich privater Lebensgestaltung,
- Beschränkung der Möglichkeiten der Zweckänderung (§ 39 Abs. 1 Satz 1 Ziffer 1 Nds. SOG),
- Eilzuständigkeit der Polizei bei der Anordnung der präventiven Telekommunikationsüberwachung (§ 33a Abs. 4 Nds. SOG),
- Sicherstellung der Benachrichtigungspflicht, auch wenn dadurch die weitere Verwendung einer Vertrauensperson (§ 36 Abs. 1) oder der weitere Einsatz einer verdeckten Ermittlerin oder eines verdeckten Ermittlers (§ 36a) gefährdet wird (§ 30 Abs. 5 S. 1 Nr. 3 Nds. SOG).

Niedersächsisches Verfassungsschutzgesetz

Auch das Niedersächsische Verfassungsschutzgesetz ist an die Anforderungen der Entscheidungen des Bundesverfassungsgerichts anzupassen. Dies gilt umso mehr, als die Arbeit des Verfassungsschutzes in noch stärkerem Maße als die der Polizei auf verdeckte Datenerhebungen ausgerichtet und zudem noch im Vorfeld der polizeilichen präventiven Zuständigkeit angesiedelt ist. Die Anpassung betrifft die folgenden Regelungsbereiche:

- Sicherstellung des absoluten Schutzes des Kernbereichs der privaten Lebensgestaltung,
- Schutz von Gesprächen im engsten Familien- oder Vertrautenkreis,
- Verbot der Rundumüberwachung,

- Verwertungsverbot bei unvermeidlichen Eingriffen in den Kernbereich privater Lebensgestaltung,
- Kennzeichnungspflicht für bestimmte Daten,
- Beschränkung der Möglichkeiten der Zweckänderung.

Niedersächsisches Ausführungsgesetz zum G 10-Gesetz
Regelungen zum Schutz des absoluten Kernbereichs privater Lebensgestaltung, zu Verwertungsverboten sowie zur Kennzeichnungspflicht sind auch hier erforderlich, sind jedoch nicht im Ausführungsgesetz, sondern im G 10-Gesetz selbst zu treffen. Hier ist daher eine entsprechende Initiative Niedersachsens erforderlich, sollte nicht der Bundesgesetzgeber von sich aus tätig werden.

Auswirkungen auf das Bundesrecht

Die beiden Entscheidungen des Bundesverfassungsgerichts haben auch erhebliche bundesrechtliche Auswirkungen in den unterschiedlichsten Bereichen. Zumindest bei folgenden Gesetzen und Regelungen muss der notwendige Änderungsbedarf geprüft werden:

- Außenwirtschaftsgesetz,
- Gesetz über das Zollkriminalamt und die Zollfahndungsämter,
- Vorschriften der §§ 100a ff. StPO zur Überwachung der Telekommunikation und des § 110a StPO zum Einsatz verdeckter Ermittler,
- Bundesverfassungsschutzgesetz, insbesondere die §§ 8, 9, 15 und 18 ff., sowie die Verweisungen auf dieses Gesetz im Gesetz über den Militärischen Abschirmdienst und im Gesetz über den Bundesnachrichtendienst,
- Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz).

Die zu einzelnen Gesetzen von der Bundesregierung bereits vorgelegten Änderungsentwürfe erfüllen noch nicht alle Vorgaben des Bundesverfassungsgerichts.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de (Aktuelles/Pressemitteilungen)
www.lfd.niedersachsen.de (Themen/Innere Sicherheit)
www.lfd.niedersachsen.de (Unser Netzwerk/DSB-Konferenz)
www.datenschutz.de (Übersicht/News)
w**ww.datenschutzzentrum.de** (Themen/Recht)
www.bfd.bund.de (Aktuelles)
www.humanistische-union (Presse)

2 Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung (Nds. SOG)

Werden verfassungsrechtliche Grenzen überschritten?

Nach ausführlichen Beratungen in den Gremien des Niedersächsischen Landtages trat am 19. Dezember 2003 das novellierte Niedersächsische Gefahrenabwehrgesetz unter dem neuen Namen „Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung" in Kraft. Es wurde als „modernstes Polizeigesetz Deutschlands" gepriesen.

Die Polizei im Vorfeld ihrer Aufgaben

Kernpunkt der Neuregelung ist aus datenschutzrechtlicher Sicht die Einführung der präventiven Telekommunikationsüberwachung in den §§ 33a bis 33c Nds. SOG. Hiermit wird der Polizei u. a. erlaubt, Daten durch Überwachung der Telekommunikation von Personen zu erheben, bei denen (nur) „Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden". Durch diese Vorschrift werden der Polizei in dem grundrechtlich geschützten Bereich des Artikels 10 des Grundgesetzes einschneidende Befugnisse eingeräumt, ohne dass das bislang im Polizeirecht immer erforderliche Merkmal der (konkreten) Gefahr vorliegen muss. Die Polizei hat damit die Möglichkeit, bereits weit im Vorfeld einer (konkreten) Gefahrenlage bzw. einer Straftat auf Grund einer Vorschrift mit sehr unbestimmten Tatbestandsmerkmalen in das grundrechtlich geschützte Fernmeldegeheimnis einzugreifen.

Art. 10 Abs. 1 GG:
„Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich."

Die unbeteiligten Dritten

Viele Bürgerinnen und Bürger müssen nunmehr damit rechnen, dass die Polizei auf Grund der Vermutung, sie selbst könnten künftig Straftaten von erheblicher Bedeutung begehen, ihre Telekommunikation überwacht. Aber der Kreis der Betroffenen reicht noch sehr viel weiter.

Für diesen zweiten Personenkreis reicht es für einen Eingriff in ihr Grundrecht aus Art. 10 GG aus, dass sie lediglich mit einer Person des ersten Personenkreises derart in Verbindung stehen, dass erwartet werden kann, dass durch sie Hinweise über angenommene Straftaten gewonnen werden können. Es reicht also, wenn die Polizei aus Ihrer Stammtisch- oder Skatrunde eine Person „im Visier" hat, um Ihre Telekommunikation gezielt zu überwachen. Und auch für all diejenigen, die einen überwachten Anschluss anrufen oder von einem überwachten Anschluss aus angerufen werden, wird ohne ihr Wissen das Fernmeldegeheimnis aufgehoben. Es stellt sich die Frage, ob für all diese Grundrechtseingriffe der Grundsatz der Verhältnismäßigkeit noch gewahrt ist.

Verfassungsbeschwerde gegen § 33a Abs. 1 Nr. 2 und 3 Nds. SOG

Ein Bürger aus Niedersachsen hat sich am 19. Februar 2004 mit einer Verfassungsbeschwerde und am 9. März 2004 mit einem Antrag auf Erlass einer einstweiligen Anordnung an das Bundesverfassungsgericht in Karlsruhe mit dem Ziel gewandt, die vorgenannten Vorschriften für verfassungswidrig erklären bzw. ihren Vollzug bis zur Entscheidung in der Hauptsache aussetzen zu lassen. Das Bundesverfassungsgericht hat auch mir Gelegenheit zur Stellungnahme gegeben. Mit Schriftsatz vom 19. August 2004 habe ich die Position des Klägers/Antragstellers gegenüber dem Bundesverfassungsgericht unterstützt. Der Entscheidung des Bundesverfassungsgericht sehe ich mit Spannung entgegen.

Wird das Trennungsgebot zwischen Polizei und Verfassungsschutz aufgehoben?

Ich hatte bereits in meinem letzten (XVI.) Tätigkeitsbericht unter der Ziffer 6.2 die gefährliche Entwicklung der letzten fünfzehn Jahre aufgezeigt, die mittlerweile durch die §§ 33a ff. Nds. SOG einen neuen Höhepunkt erreicht hat. Durch die Aufgaben- und Befugnisverlagerung in das Vorfeld von Gefahren und Straftaten läuft die Polizei Gefahr, sich so weit von ihren klassischen Aufgaben der Gefahrenabwehr und Strafverfolgung zu entfernen, dass man ihre Aufgaben und ihre Befugnisse demnächst nicht mehr von denen des Verfassungsschutzes wird unterscheiden können.

Die Alliierten und der Grundgesetzgeber wollten jedoch mit Hilfe des Trennungsgebotes ein Wiederaufleben polizeilicher Kompetenzzusammenballungen, wie sie zu Zeiten des „Dritten Reiches“ das Reichssicherheitshauptamt und die Gestapo hervorgebracht haben, für alle Zukunft verhindern. Das Trennungsgebot ist durch unser Grundgesetz (Art. 73 und 87 GG) in Verbindung mit dem sog. Polizeibrief der Alliierten Militärgouverneure vom 14. April 1949 und das Genehmigungsschreiben der Militärgouverneure der britischen, französischen und amerikanischen Besatzungszone zum Grundgesetz vom 12. Mai 1949 festgeschrieben.

Es ist inzwischen, insbesondere durch Gesetzesänderungen, die nach dem 11. September 2001, aber auch schon vorher, zur Bekämpfung der organisierten Kriminalität eingefordert wurden, allerdings derart aufgeweicht worden, dass es de facto kaum noch existiert, eine Entwicklung, die ich mit allergrößter Sorge betrachte.

Vertiefende Informationen zum Thema:

Zur Präventiven Telekommunikationsüberwachung:

www.lfd.niedersachsen.de
(Themen/Innere Sicherheit)

www.datenschutz.hessen.de
(Auswahlmenue/Tätigkeitsberichte/30. TB/9.1)

Zum Trennungsgebot des Grundgesetzes:

Kutscha in ZRP 1986, 194 ff. und Gusy in ZRP 1987, 45 ff.

Die DNA-Analyse im Strafverfahren 3

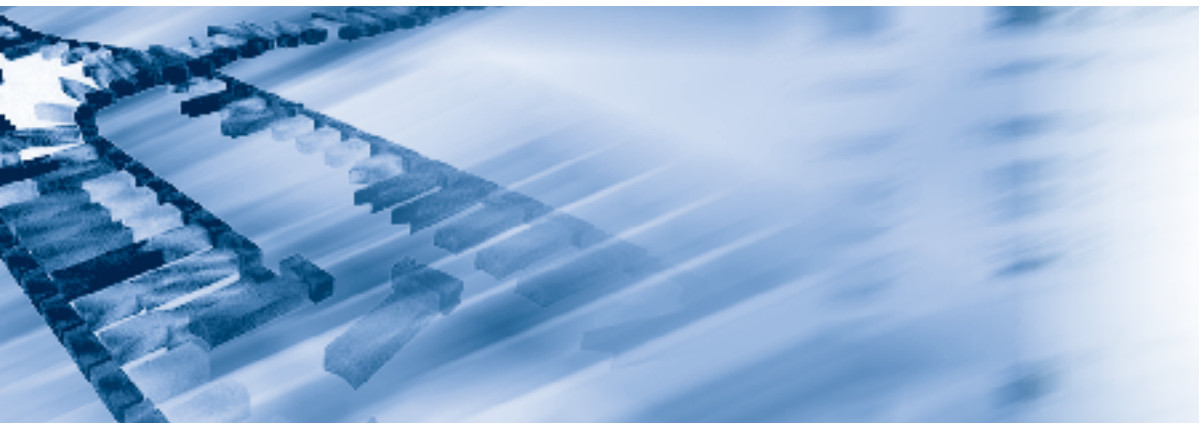
Der genetische Fingerabdruck als Standardinstrument der erkennungsdienstlichen Behandlung?

Die Forderung, den so genannten „genetischen Fingerabdruck" als normale erkennungsdienstliche Maßnahme freizugeben und dafür die derzeit bestehenden engen gesetzlichen Anforderungen zu lockern, wird von Teilen der Polizei und der Politik immer vehementer erhoben. Die Erfassung und Speicherung des „genetischen Fingerabdrucks" von Straftätern soll genauso einfach möglich sein, wie es beim klassischen Fingerabdruck der Fall ist. Sowohl die Justizministerkonferenz als auch die Innenministerkonferenz haben sich mit den Ausweitungsmöglichkeiten der DNA-Analyse befasst und entsprechende gesetzgeberische Aktivitäten empfohlen. Neben der rechtlichen Gleichsetzung mit dem herkömmlichen Fingerabdruck geht es insbesondere auch um den Verzicht auf den sogenannten Anlasstatenkatalog, wie er z.z. noch im geltenden § 81g StPO vorgesehen ist.

Was spricht dagegen?

Dass die DNA-Analyse ein hoch wirksames Ermittlungsinstrument bei der Aufklärung von Straftaten ist, ist unbestreitbar. In der öffentlichen Diskussion sind schon von daher Vorbehalte gegen eine Erweiterung ihres derzeitigen Anwendungsbereiches nur schwer zu vermitteln. Gleichwohl haben die Datenschutzbeauftragten des Bundes und der Länder mit ihrer Entschließung vom 16.07.2003 darauf gedrungen, bei der Erweiterung der DNA-Analyse Augenmaß zu bewahren und sie nicht zu einem Routinewerkzeug einer jeden erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument werden zu lassen.

Es darf insbesondere nicht außer Acht gelassen werden, dass die DNA-Analyse einen tiefen Eingriff in das Recht auf informationelle Selbstbestimmung bedeutet. Denn anders als beim klassischen Fingerabdruck lassen sich aus dem „genetischen Fingerabdruck" über den reinen Sequenzabgleich mit dem Referenzmaterial hinaus in erheblichem Umfang Zusatzinformationen gewinnen, die sehr wohl persönlichkeitsrelevant sind. Selbst wenn bisher nur sog. nicht codierende Gensequenzen erfasst werden, lassen sich hieraus bereits Aussagen über das Geschlecht, über Wahrscheinlichkeiten von Verwandtschaften und von ethnischen Zugehörigkeiten sowie – derzeit noch sehr eingeschränkt – von Krankheiten treffen. Durch die Wortwahl „genetischer Fingerabdruck" wird die andere Eingriffsqualität der DNA-Analyse – bewusst oder unbewusst – ausgeblendet. Dieselbe Verharmlosung findet sich, wenn der Eingriff in die Persönlichkeitsrechte auf ein „Lecken am Holzstäbchen" reduziert wird.



§ 81g StPO:
„Zum Zwecke der Identitätsfeststellung (…) dürfen dem Beschuldigten, der einer Straftat von erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung, eines Diebstahls in einem besonders schwerem Fall oder einer Erpressung verdächtig ist, Körperzellen entnommen und (…) molekulargenetisch untersucht werden."

Verfassungsrechtliche Anforderungen

Alle Maßnahmen zur Ausweitung der DNA-Analyse im Strafverfahren müssen sich deshalb aus meiner Sicht auch weiterhin an den Anforderungen des Bundesverfassungsgerichtes orientieren. Notwendig für die Anordnung der Maßnahme ist daher, dass wegen der Art oder Ausführung der bereits abgeurteilten Straftat, der Persönlichkeit des Verurteilten oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass gegen ihn künftig erneut Strafverfahren wegen Straftaten von erheblicher Bedeutung zu führen sind. Dies setzt eine Prognoseentscheidung voraus, die im Hinblick auf die Gefahr der Wiederholung auf schlüssigen, verwertbaren und in der Entscheidung nachvollziehbar dokumentierten Tatsachen beruhen muss. Auf dieser Grundlage setzt die richterliche Entscheidung über die Annahme der Wahrscheinlichkeit künftiger Straftaten von erheblicher Bedeutung auf. Die Anordnung zur Entnahme von Körperzellen darf nur erfolgen, wenn das DNA-Identifizierungsmuster einen Aufklärungsansatz durch einen (künftigen) Spurenvergleich bieten kann.

Ein Wegfall der Erheblichkeitsschwelle bzw. eine Ausweitung auf Bagatelldelikte würde dem in den Entscheidungen des Bundesverfassungsgerichtes hervorgehobenen Verhältnismäßigkeitsgrundsatz zuwiderlaufen. Am logischen Ende dieser Entwicklung würde eine lückenlose Erfassung und fortdauernde Speicherung der DNA-Identifizierungsmuster der gesamten erwachsenen (oder auch schon der heranwachsenden?) Bevölkerung stehen. Damit würde man zwar optimale Bedingungen für die Aufklärung von Straftaten schaffen, gleichzeitig würde aber jeder unter einen Generalverdacht als potentieller künftiger Straftäter gestellt, was mit den Grundsätzen unseres Rechtsstaats und der Unschuldsvermutung völlig unvereinbar wäre.

Ich werde die Diskussion um die Ausweitung der DNA-Analyse weiterhin sehr genau verfolgen und darauf dringen, dass die aus dem GG hergeleiteten Anforderungen des Bundesverfassungsgerichts strikt eingehalten werden. Dazu gehört auch die Aufrechterhaltung angemessener Kontrollmechanismen (Richtervorbehalt).

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de
(Themen/Biometrie/DNA-Analyse)

www.lfd.niedersachsen.de
(Aktuelles/Pressemitteilungen)

www.datenschutz-berlin.de
(Deutschland/Konferenz der Datenschutzbeauftragten/Entschließungen zwischen der 65. und 66. Konferenz)

Bundesverfassungsgericht:
2 BvR 1741/99, 2 BvR 276/00,
2 BvR 2061/00 vom 14.12.2000
und 2 BvR 2232/00 vom 20.12.2000

www.bverfg.de
(Entscheidungen)

Auszug „Steueränderungsgesetz 2003“
vom 15.12.2003 (BGBl I S. 2645 ff.)

§ 139a Abgabenordnung
Identifikationsmerkmal
(1) Das Bundesamt für Finanzen teilt jedem Steuerpflichtigen zum Zwecke der eindeutigen Identifizierung in Besteuerungsverfahren ein einheitliches und dauerhaftes Merkmal (Identifikationsmerkmal) zu, das bei Anträgen, Erklärungen oder Mitteilungen gegenüber Finanzbehörden anzugeben ist. Es besteht aus einer Ziffernfolge, die nicht aus anderen Daten über den Steuerpflichtigen gebildet oder abgeleitet werden darf; die letzte Stelle ist eine Prüfziffer. Natürliche Personen erhalten eine Identifikationsnummer, …

Einheitliches Personenkennzeichen 4

„Personenkennzeichen“? – Doch nicht bei uns!

Der Mensch eine Nummer – in Dänemark oder Schweden mag das so sein, aber doch nicht in Deutschland! Wer dies immer noch so sieht, hat die jüngste Entwicklung nicht verfolgt. Dabei bestand bis vor kurzem in Politik und Gesellschaft noch weitgehend Konsens darüber, dass ein einheitliches fachübergreifendes Personenkennzeichen mit dem Grundrecht auf informationelle Selbstbestimmung nicht zu vereinbaren ist. Dies ist auch die Auffassung des Bundesverfassungsgerichts, die es schon in seinem „Volkszählungsurteil“ vom 15.12.1983 vertreten hat. Hiernach sind unzulässige Persönlichkeitsbilder zu erwarten, „soweit eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre“ (BVerfGE 65, 1, 53; NJW 1984, 419, 424). Daher ist das in der ehemaligen DDR bis zur „Wende“ gebräuchliche Personenkennzeichen, das zur Erschließung der zentralen Einwohnerregister verwendet wurde, unverzüglich mit Wiederherstellung der deutschen Einheit abgeschafft worden.
Darüber hinaus galt der Grundsatz, dass auch die in den verschiedensten Aufgabenbereich eingesetzten numerischen Ordnungsmerkmale – etwa die mit dem Personalausweis verbundene Ausweisnummer – grundsätzlich keine Rückschlüsse auf Personen zulassen dürfen und in jedem Falle hinsichtlich ihrer Nutzung und Zweckbindung sehr engen Restriktionen unterliegen (so z. B. bei der Sozialversicherungsnummer).

Die Personenkennziffer – und sie lebt doch!

Tatsächlich hat aber Ende der 90er-Jahre eine Entwicklung eingesetzt, die Akzeptanz für die Einführung zentral auswertbarer Ordnungsnummern zu schaffen suchte. Die Kapazitäten der heute einsetzbaren Datenbanken und die Möglichkeiten der Verknüpfung und Auswertung der an vielen Stellen überreich vorhandenen Datenbestände verleiten zu solchen Überlegungen. Die Gründe für die Einführung einheitlicher Kennziffern sind vielfältig und für sich genommen

auch durchaus nachvollziehbar. Wer könnte schon etwas dagegen haben, wenn durch eine „Personenkennziffer" etwa alle in Personalausweisen und Pässen enthaltenen und in einer zentralen Datei hinterlegten biometrischen Merkmale rasch und zuverlässig erschlossen und so die Möglichkeiten der Polizei- und Sicherheitsbehörden zur Verfolgung der organisierten Kriminalität oder zur Terrorbekämpfung verbessert werden sollen?

Identifikationsnummer – „Der gläserne Steuerzahler!"

Entsprechendes gilt für die Bekämpfung der Schwarzarbeit oder der Steuerhinterziehung. So hat der Bundesgesetzgeber, von der Öffentlichkeit kaum registriert, in das so genannte „Steueränderungsgesetz 2003" eine Regelung eingefügt, nach der künftig jedem steuerpflichtigen Einwohner, schon den Neugeborenen, ein numerisches Identifikationsmerkmal zugeteilt werden soll, das zentral beim Bundesamt für Finanzen und darüber hinaus parallel auch in den kommunalen Meldeämtern gespeichert wird („Identifikationsnummer"). Durch die zentrale Speicherung der Identifikationsnummer sollen der Informationsfluss und damit auch Datenabgleiche innerhalb der Finanzverwaltung erleichtert, das Besteuerungsverfahren effizienter gestaltet und somit ein wesentlicher Beitrag zur Steuergerechtigkeit geleistet werden. Die Frage, ob wirklich jeder Einwohner als potentieller Steuerhinterzieher unter „Generalverdacht" gestellt werden muss und nicht vielmehr zunächst die bisherigen Möglichkeiten besser ausgeschöpft und Verfahrenabläufe effizienter gestaltet werden sollten, wird allenfalls am Rande erörtert. Im Ergebnis wird alsbald erstmals in der Geschichte der Bundesrepublik Deutschland mit dem Bundesamt für Finanzen eine zentrale Stelle über die Grunddaten aller 80 Millionen Einwohnerinnen und Einwohner (beispielsweise Familienname, frühere Namen, Vornamen, Geburtsdatum, Geburtsort, Anschrift) verfügen. Auch wenn diese Daten nach den derzeitigen gesetzlichen Regelungen nur für steuerliche Zwecke genutzt werden dürfen, bleibt zu befürchten, dass dieser „Datenpool" auch außerhalb der Finanzverwaltung Begehrlichkeiten wecken und sehr bald der Wunsch an den Gesetzgeber herangetragen werden wird, diese Datenbestände auch für andere Verwaltungsbereiche zu erschließen.

Auszug „Steueränderungsgesetz 2003" vom 15.12.2003 (BGBl I S. 2645 ff.)

§ 139b Abgabenordnung

(6) Zum Zwecke der erstmaligen Zuteilung der Identifikationsnummer übermitteln die Meldebehörden dem Bundesamt für Finanzen 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.

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 § 5 des Einführungsgesetzes zur Abgabenordnung bestimmt wird. Das Bundesamt für Finanzen teilt der zuständigen Meldebehörde die dem Steuerpflichtigen zugeteilte Identifikationsnummer zur Speicherung im Melderegister mit.

(7) Die Meldebehörden haben im Falle der Speicherung einer Geburt im Melderegister sowie im Falle der Speicherung einer Person, für die bisher keine Identifikationsnummer zugeteilt worden ist, dem Bundesamt für Finanzen die Daten nach Absatz 6 Satz 1 zum Zwecke der Zuteilung der Identifikationsnummer zu übermitteln. Absatz 6 Satz 2 und 3 gilt entsprechend.

(8) Die Meldebehörde teilt dem Bundesamt für Finanzen Änderungen der in Absatz 6 Satz 1 Nr. 1 bis 8 bezeichneten Daten sowie bei Sterbefällen den Sterbetag unter Angabe der Identifikationsnummer mit.

Appell der Datenschutzbeauftragten: Personennummern vermeiden!

Die Konferenz der Datenschutzbeauftragten hat sich auf Grund der aus datenschutzrechtlicher Sicht problematischen Entwicklung mehrfach mit der Thematik befasst und an die Gesetzgeber appelliert, solche Personennummern zu vermeiden. Soweit im Einzelfall in bestimmten Aufgabenbereichen derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

Vertiefende Informationen zum Thema:

www.datenschutz.de und www.datenschutz.hessen.de
jeweils unter dem Stichwort „Personenkennzeichen"

Neue Personalverwaltungssysteme 5

Droht der „Gläserne Bedienstete“?

In der Landesverwaltung, im Hochschulbereich und in vielen Kommunen werden derzeit neue programmgestützte Personalverwaltungssysteme eingeführt. Vielfach werden hierbei auch technisch überholte und unter dem Aspekt der Datensicherheit problematische Verfahren durch moderne Softwareprodukte ersetzt. Diese neuen Personalwaltungssysteme steigern nicht nur die Effizienz der Personalbearbeitung erheblich, sie bieten im Vergleich zu den bisherigen Systemen auch vielfältige Möglichkeiten der Verknüpfung und gezielten Auswertung von Personaldaten. Hieraus ergibt sich die Befürchtung bei vielen Beschäftigten und Personalräten, dass der „Gläserne Bedienstete“ Realität wird.

Personalmanegementverfahren (PMV)

Für die unmittelbare Landesverwaltung soll ein landeseinheitliches Personalmanagementverfahrens (PMV) eingesetzt werden, das letztlich die Personaldaten von ca. 200.000 Beschäftigten verarbeiten und über Schnittstellen mit anderen Verfahren (Auszahlung der Bezüge, Haushaltsbewirtschaftung) verknüpft werden soll. Das federführende Finanzministerium hat mich bereits im Vorfeld bei der Auswahl und später auch bei den vorbereitenden Arbeiten zur Einführung des neuen Verfahrens beteiligt.

Anforderungen für eine datenschutzgerechte Ausgestaltung

Im Zusammenwirken mit den Gewerkschaften und Personalvertretungen habe ich Anforderungen für eine datenschutzgerechte Ausgestaltung des Personalmanagementverfahrens entwickelt, die auch Eingang in die zur Einführung des Verfahrens abgeschlossene Vereinbarung nach § 81 NPersVG gefunden haben. Die wichtigsten Eckpunkte für eine datenschutzgerechte Ausgestaltung, die in gleicher Weise auch für andere eingesetzte Programme, z. B. SAP H/R Geltung beanspruchen, sind die folgenden:

- Im PMV dürfen grundsätzlich nur die Personaldaten verarbeitet werden, die für eine effiziente und effektive Personalverwaltung und -wirtschaft erforderlich sind. Der Katalog der Personaldaten, die landeseinheitlich verbindlich für alle Beschäftigten erfasst werden, ist auf das erforderliche Maß zu begrenzen und zentral zu definieren. Zusätzliche bereichsspezifische Datenbankfelder dürfen nur eingerichtet werden, soweit dies auf Grund von Besonderheiten in den jeweiligen Aufgabenbereichen (z. B. der Polizei, der Schulverwaltung) erforderlich ist (Grundsatz der Erforderlichkeit sowie der Datenvermeidung und Datensparsamkeit).

- Die Betroffenen sind über ihren persönlichen Datenbestand zeitnah nach der Erfassung und bei nachfolgenden Änderungen zu unterrichten. Hierzu erhalten sie einen Ausdruck ihres persönlichen Datenbestandes. Im Zuge der Vervollständigung des Verfahrens ist ein individueller Zugriff auf die persönlichen Daten vorzusehen. Beschäftigte haben grundsätzlich das Recht der jederzeitigen vollständigen Information über alle in Bezug auf ihre Person gespeicherten Daten (Transparenzgebot).
- Auswertungen des Personaldatenbestandes unterliegen einer engen personalwirtschaftlichen Zweckbindung. Der Katalog der zulässigen Auswertungen wird zentral oder in ressortspezifischen Vereinbarungen festgelegt. Die Auswertungen sind zu einem frühestmöglichen Zeitpunkt zu anonymisieren.
  Datenbankfelder ohne konkrete personalwirtschaftliche Zweckbindung sind unzulässig. Ein Zugriff auf den Personaldatenbestand und personenbezogene Auswertungen sind nur zulässig, soweit dies im Rahmen der Aufgabenerfüllung erforderlich ist. Hierfür ist ein Berechtigungs- und Zugriffskonzept zu erstellen. Entsprechendes gilt für die Administration des Verfahrens.
- Die Zugriffe auf das Verfahren sind in geeigneter Weise zu protokollieren und regelmäßig zu kontrollieren.
- Der Datenaustausch über Schnittstellen zu anderen Verfahren, etwa zum Bezügeverfahren oder in die Kosten- und Leistungsrechnung, ist inhaltlich und technisch zu dokumentieren.
- Die Vertraulichkeit, Integrität und Authentizität der Daten ist durch geeignete technisch-organisatorische Maßnahmen abzusichern. Für die Datenübertragung ist zur Gewährleistung der Vertraulichkeit eine geeignete Verschlüsselung vorzusehen. Die Clients sollten zur Authentisierung mit Chipkartenbasierten Zertifikaten ausgestattet werden.
- Die Datenschutz- und Datensicherungsmaßnahmen sind an den Ergebnissen der Vorabkontrolle auszurichten und im Zuge der notwendigen Anpassungen und Veränderungen des Verfahrens dem Stand der Technik entsprechend fortzuentwickeln („Technikfolgencontrolling").

Bei der jetzt anstehenden Pilotierung im Bereich der Landespolizei werde ich darauf achten, dass die datenschutzrechtlichen Vorgaben aus der Vereinbarung nach § 81 NPersVG, insbesondere zur Gewährleistung von Vertraulichkeit, Integrität und Authentizität der im PMV verarbeiteten Personaldaten, sowie die nach dem Ergebnis der Vorabkontrolle erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit auch tatsächlich umgesetzt werden.

Allen Personalvertretungen und Bediensteten stehe ich darüber hinaus gerne zur Beratung zur Verfügung.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de unter dem Pfad > Home > Themen > PMV
www.nlbv.de unter dem Pfad „Projekt PMV"

Betriebswirtschaftliche Steuerungsinstrumente (Kosten- und Leistungsrechnung)

Bleibt der Personaldatenschutz auf der Strecke?

Wie teuer ist eigentlich „der Datenschutz"? Was kostet der Unterhalt eines Kindergartens oder die Erteilung einer Gaststättenerlaubnis? Stehen Aufwand und Nutzen in einem angemessenen Verhältnis? Werden die Personalressourcen und Sachmittel zielgerichtet und effizient eingesetzt? „LoHN"t sich das überhaupt?

Aus dem bisherigen Haushaltsbewirtschaftungssystem erschließen sich solche Erkenntnisse jedenfalls nicht. Die politisch Verantwortlichen und die Bürgerinnen und Bürger haben aber ein Anrecht darauf, zu erfahren, in welcher Höhe Steuermittel für den Betrieb eines Kindergartens, für die Aufklärung eines Verbrechens oder auch für den Datenschutz eingesetzt werden und was mit den eingesetzten Mitteln tatsächlich erreicht wurde. Dazu müssen selbstverständlich auch die Behördenleitungen mit Informationen versehen werden, damit sie durch Zielvorgaben und Steuerung den Mitteleinsatz und die Arbeitsergebnisse optimieren können.

Transparenz auf der Kostenseite – muss das sein?

Das kameralistische Haushaltssystem weist zwar die Einnahmen und Ausgaben differenziert nach, kann aber eine Zuordnung von Finanzmitteln zu einzelnen Leistungen und Ergebnissen nicht darstellen. Dies gilt selbstverständlich auch für die Aufgabenerledigung des Landesbeauftragten für den Datenschutz und der zugeordneten Geschäftsstelle. So war ich bisher kaum in der Lage, Aufwand und Kosten den einzelnen Aufgaben konkret zuzuordnen. Ich habe mich deshalb dem in der Landesverwaltung laufenden Projekt „Leistungsorientierte Haushaltswirtschaft Niedersachsen (LoHN)" angeschlossen und auch in meiner Geschäftstelle eine Kosten- und Leistungsrechung (KLR) auf der Basis des Systems Baan eingeführt.

KLR = „Der gläserne Mitarbeiter" – stimmt das?

Wie in vielen anderen Dienststellen begegneten auch meine Mitarbeiterinnen und Mitarbeiter dem Projekt teils zurückhaltend, teils skeptisch. Man vermutete, durch zu detaillierte Erhebungen und das auf die Ergebnisse eines „Berichtswesens" aufsetzende „Controlling" zu transparent, also zum „gläsernen Mitarbeiter" zu werden. Vor allem bestand die Sorge, dass die Ergebnisse aus der KLR letztlich doch zu einer individuellen Verhaltens- und Leistungskontrolle genutzt werden könnten.

Diese Bedenken sind durchaus nachvollziehbar, aber im Ergebnis nicht begründet. Auch für mich ist klar, dass sich die Effizienz eines Mitarbeiters nicht nur an „Kennzahlen" messen lässt. Um diesen und anderen Bedenken zu begegnen, bedurfte es sowohl einer umfassenden Information der Mitarbeiterinnen und Mitarbeiter über die Ziele und den Nutzen des Verfahrens als auch einer konsequenten Umsetzung der datenschutzrechtlichen Vorgaben.

6

KLR in der Geschäftsstelle des LfD – ja, aber datenschutzgerecht!

Für mich war es daher selbstverständlich, die datenschutzrechtlichen Vorgaben im eigenen Bereich konsequent und zielgenau umzusetzen, die ich zur Einführung der betriebswirtschaftlichen Steuerungsinstrumente in der Landesverwaltung in engem Zusammenwirken mit den Gewerkschaften erarbeitet hatte und die Eingang in die Vereinbarung nach § 81 NPersVG gefunden hatten (vgl. XVI. TB, 9.3). So habe ich zur Einführung der KLR und der automatisierten Zeiterfassung eine Dienstvereinbarung nach § 78 NPersVG mit dem Personalrat über die Verwendung von pseudonymen und jährlich wechselnden Identifikationsnummern und den Einsatz von Vertrauenspersonen abgeschlossen; hierdurch wird eine zu weitgehende Transparenz des einzelnen Beschäftigten verhindert. Darüber hinaus sind auch die Rollen- und Rechteprofile der KLR-Administratoren und der in das Verfahren eingebundenen Vorgesetzten eindeutig definiert worden. Wie ich selbst festgestellt habe, ist allerdings in kleinen Dienststellen die Wirkung derartiger Maßnahmen schon deshalb beschränkt, weil hier auf Grund der sehr engen Arbeitskontakte in erheblichem Umfang Zusatzwissen entsteht, das auch durch noch so ausgefeilte Regelungen zur Anonymisierung und Abschottung nicht ausgeschaltet werden kann.

Ständiges „Datenschutzcontrolling“ ist notwendig!

Der weitere Einsatz der neuen betrieblichen Steuerungsinstrumente in der Landesverwaltung bedarf meiner ständigen Begleitung. Hierbei wird unter Berücksichtigung der praktischen Erfahrungen in den Dienststellen zu prüfen sein, ob und inwieweit die datenschutzrechtlichen Vorgaben in der Praxis ihren Zweck erfüllen oder möglicherweise einen effizienten Einsatz der neuen Steuerungsinstrumente im Einzelfall zu sehr behindern. Ich stehe allen Beteiligten, insbesondere auch den Verantwortlichen in den Dienststellen und den Personalvertretungen, für eine ergebnisoffene Diskussion und zur Beratung weiterhin zur Verfügung.

Vertiefende Informationen zum Thema:

www.mf.niedersachsen.de
Themen/Verwaltung/Kosten-Leistungs-rechnung

JobCard-Verfahren 7

Wie können Arbeitnehmerdaten dabei vor unberechtigten Zugriffen geschützt werden?

Die JobCard mit der zentralen Speicherung von Arbeitnehmerda
Hartz-Konzepts zur Reform des Arbeitsmarktes. Die Bundesregierung verfolgt mit der Einrichtung einer zentralen Annahmestelle für das Bescheinigungswesen das Ziel, den Einsatz der Signaturkarte durch Anwendungen in der Praxis zu fördern. Sie soll verpflichtend für alle Arbeitnehmer und Beamte eingeführt werden und den elektronischen Zugriff auf bei einer zentralen Stelle gespeicherte Daten (z. B. Beschäftigungsbeginn, Entgeltzahlungen, Ende des Beschäftigungsverhältnisses) ermöglichen. Dazu werden die Arbeitgeber die Daten der Arbeitnehmer monatlich bzw. bei Beendigung des Beschäftigungsverhältnisses an die zentrale Stelle auf elektronischem Wege verschlüsselt übermitteln. Zuvor muss jeder Arbeitnehmer einen Antrag bei einer Registrierungsstelle einreichen und sich hierbei durch persönliches Erscheinen legitimieren. Durch den genehmigten Antrag wird er für das JobCard-Verfahren zugelassen. Die zentrale Stelle „Registratur Fachverfahren" stellt die Verknüpfung zwischen der Identitätsnummer der JobCard und der Sozialversicherungsnummer des Arbeitnehmers her. Sendet ein Arbeitgeber die Daten verschlüsselt an die zentrale Speicherstelle, werden sie verschlüsselt nach dem Ordnungskriterium Sozialversicherungsnummer abgelegt. Benötigt dann z. B. ein Mitarbeiter der Arbeitsagentur die Daten des Arbeitnehmers für die Bearbeitung eines Antrages auf Arbeitslosengeld, muss der Antragsteller unter Nutzung seiner JobCard als Signaturkarte in den Abruf der Daten einwilligen. Zusätzlich muss sich der Mitarbeiter der Arbeitsagentur durch Einsatz seiner Signaturkarte legitimieren.
Durch dieses Verfahren sollen die Verwaltungsabläufe der Arbeitsagenturen, Sozialversicherungsträger und Kommunen deutlich beschleunigt und einkommens- oder lohnabhängige Sozialleistungen schneller erbracht werden können. Die jährliche Einsparung für die Arbeitgeber wird auf 500 Mio. Euro geschätzt. Starten soll das JobCard-Verfahren zum 01.01.2007.

Reichen die bisherigen Vorkehrungen zur Gewährleistung von Datenschutz und Datensicherheit aus?

Mit Hilfe moderner Kommunikationstechnik werden durch das JobCard-Verfahren erstmals Millionen von Arbeitnehmerdaten bei einer zentraler Stelle gespeichert. Ob überhaupt, wann, wie oft und zu welchem Zweck diese Daten später einmal zur Bearbeitung eines Vorgangs bei der Arbeitsagentur, bei einem Sozialversicherungsträger oder bei einer Kommune gebraucht werden, ist im

Zeitpunkt ihrer Übermittlung an die zentrale Speicherstelle völlig ungewiss. Die Übermittlung und Speicherung geschieht also gewissermaßen auf Vorrat. Zu der Datenspeicherung auf Vorrat hat das Bundesverfassungsgericht in seiner grundlegenden Entscheidung zum Volkszählungsgesetz 1983, in welchem es aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG das Recht auf informationelle Selbstbestimmung abgeleitet hat, ausgeführt:

„Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren".

Vor diesem Hintergrund ist zu prüfen, ob es sich beim JobCard-Verfahren um eine unzulässige Vorratsdatenhaltung handelt. Auf jeden Fall müssen verlässliche Mechanismen vorhanden sein, die einen unbefugten Zugriff definitiv ausschließen. Dazu muss insbesondere noch geklärt werden, ob auch der zentralen Speicherstelle eine Zugriffsmöglichkeit eingeräumt werden kann oder ob nicht ohne eine solche Zugriffsmöglichkeit durch eine Ende-zu-Ende-Verschlüsselung die alleinige Verfügungsbefugnis des Arbeitnehmers über seine Daten konsequent verwirklicht werden muss. Die Zentrale Speicherstelle verfügt schließlich bei Umsetzung des JobCard-Verfahrens über Entgeltdaten aller in Deutschland beschäftigten Arbeitnehmer und Beamten für jeweils rund 10 zurückliegende Jahre. Erst dann erfolgt die Löschung, da Leistungen auch noch für vergangene Jahre beantragt werden können. Gerade deshalb ist ein erhöhter Sicherheitsbedarf für die Verarbeitung und Speicherung der Daten in der ZSS vorzusehen. Mit der Klärung dieser und anderer noch offener Fragen des Datenschutzes befasst sich eine Arbeitsgruppe der Datenschutzbeauftragten, an der auch ich intensiv beteiligt bin. Ziel bleibt es, dass das Recht auf informationelle Selbstbestimmung der Arbeitnehmer auch beim JobCard-Verfahren konsequent durchgesetzt wird.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de
(Themen, Sozialdaten)

www.datenschutz.de
(Recht, Gesundheitswesen)

www.datenschutzzentrum.de
(material/themen/jobcard/)

www.bfd.bund.de
(Materialien zum Datenschutz/Tätigkeitsberichte/19. TB/Nr. 23.2.2)

DuD, Datenschutz und Datensicherheit (2004), S. 404
Computerzeitschrift C't Heft 13 2004, S. 46 und S. 49

Die elektronische Gesundheitskarte (eGK) 8

Die Weichen sind gestellt!

Spätestens zum 01.01.2006 sollen alle 70 Millionen in der gesetzlichen Krankenversicherung Versicherten Leistungen unter Einsatz der eGK erhalten. Auch wenn der im Gesetz genannte Termin aus heutiger Sicht sehr ehrgeizig erscheint, werden die Versicherten zumindest zu diesem Termin eine neue Krankenversicherungskarte mit Lichtbild erhalten.
Die Einführung der eGK gilt als das derzeit weltweit größte IT-Projekt.

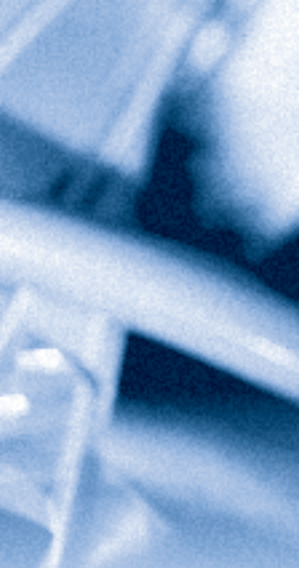
Zusätzlich zu den bisher auf der Krankenversicherungskarte vorhandenen persönlichen Daten des Versicherten (z. B. Name, Vorname, Krankenversicherungsnummer, Krankenkasse) werden in einem elektronischen Chip auf der eGK das so genannte elektronische Rezept und der Zuzahlungsstatus gespeichert und es wird der Berechtigungsausweis nach dem Recht der Europäischen Union auf der Rückseite der Karte abgebildet. Neben diesen Pflichteintragungen besteht die Möglichkeit, mit einer zu dokumentierenden Einwilligung des Versicherten weitere für ihn wichtige Gesundheitsdaten (Medikation, Diagnosen, Arztberichte, Röntgenbilder usw.) elektronisch zu speichern. Diese zusätzlichen Daten sind mit einer PIN besonders geschützt und können nur von dem Versicherten freigegeben werden. Auch der Zugriff auf die Pflichtdaten der eGK erfordert in jedem Fall die einwilligende Mitwirkung des Versicherten.

Die für die Ausgestaltung der elektronischen Gesundheitskarte zuständigen Spitzenverbände von Krankenkassen, Ärzten und Apothekern haben sich darauf verständigt, innerhalb von Pilotprojekten zu testen, ob die Gesundheitsdaten vorzugsweise auf der eGK gespeichert werden sollen oder ob eine zentrale Serverlösung die bessere Alternative darstellt. Beide Varianten sollen während der in mehreren Bundesländern geplanten Testphase erprobt werden. Wichtigstes Kriterium ist dabei die Datenhoheit des Patienten.

Neben elf weiteren Bundesländern soll in Niedersachsen unter dem Namen „eHealthProjekt Wolfsburg" der Einsatz der elektronischen Gesundheitskarte erprobt werden. Beteiligt sind hier die Firmen Wolfsburg AG, Orga, DocExpert und IBM sowie die ca. 109.000 Mitglieder der Deutschen BKK.

Die eGK soll dazu beitragen, Qualität und Sicherheit der Behandlung durch bessere Verfügbarkeit behandlungsrelevanter Patientendaten und bessere Kommunikation zwischen den Beteiligten zu steigern. Daneben soll die elektronische Speicherung die Abrechnung mit den einzelnen Leistungserbringern effizienter gestalten. Jährlich werden Einsparungen von 500 bis 700 Millionen Euro bei umfassender elektronischer Nutzung erwartet.

Sofern Leistungserbringer (z. B. Ärzte und Krankenhäuser) auf die Daten der eGK zugreifen wollen, benötigen sie eine Berechtigungskarte, die sog. Health Professional Card (HPC). Nur dieser elektronische Heilberufeausweis berechtigt, auf die eGK eines gesetzlich Versicherten zuzugreifen. Die HPC soll als optischer



Das Erheben, Verarbeiten und Nutz
elektronischen Gesundheitskarte ist nur mit dem Einverständnis
der Versicherten zulässig. (§ 291a Abs. 5 Sozialgesetzbuch Teil V)

Sichtausweis wie auch als offizieller Arzt- bzw. Berufsausweis ausgegeben werden und ist bereits für Pilotprojekte freigegeben. Mit einer HPC wird außerdem der Zweck verfolgt, medizinische elektronische Dokumente sowohl im Verfügungsbereich des Leistungserbringers, vor allem aber auch außerhalb dieses Bereiches zuverlässig zu verschlüsseln und zu signieren.

Wird der „Gläserne Patient" Wirklichkeit?

Datenschutzrechtlich ist die Abspeicherung von Informationen auf einer eGK als mobilem Speichermedium schon deshalb problematisch, weil Gesundheitsdaten als besonders sensitive Daten einem erhöhten Schutz unterliegen. Dass etwa Arbeitgeber oder Versicherungen nur zu gerne auf die Daten der eGK zugreifen würden, ist offensichtlich. Um so wichtiger ist es, in der Ausgestaltung der gesamten Telematikinfrastruktur durch geeignete Schutzmechanismen sicher zu stellen, dass die Vertraulichkeit der Daten in vollem Umfang erhalten bleibt und ein Auslesen der Daten durch unberechtigte Dritte verlässlich verhindert wird. Der Gesetzgeber hat dazu bereits verbindlich vorgegeben, dass der Zugriff auf die Daten nur über eine Freischaltung der eGK durch den Versicherten einerseits und die elektronische Authentisierung des Zugreifenden über eine Signatur andererseits ausgelöst werden kann. Aus Datenschutzsicht besteht zudem die Forderung, dass die weiter notwendigen Sicherheitsfunktionen, etwa zur Sperrung des Zugriffs auf bestimmte auf der eGK gespeicherte Datenbestände durch den Versicherten, direkt auf der Karten-Betriebssystemebene realisiert werden müssen, damit alle Optionen für die künftige Sicherheitsinfrastruktur zur Verfügung stehen.

Die Datenschutzbeauftragten des Bundes und der Länder sind durch eine Arbeitsgruppe an den Planungen zur weiteren Ausgestaltung der eGK und der Telematikinfrastruktur beteiligt. Das Patienteninteresse und die Gewährleistung ihres Rechts auf informationelle Selbstbestimmung haben dabei oberste Priorität.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de
(Themen/Sozialdaten)

www.datenschutz.de
(Recht/Gesundheitswesen)

DuD, 2004, S. 391 ff.
Deutsches Ärzteblatt, Jg. 101, Heft 30, 2004, S. 2102 ff.

Datenschutz in der Arztpraxis 9

Eine gemeinsame Aktion mit den Ärztekammern, dem Gesundheitsministerium und Verbänden zur Verbesserung des Datenschutzes

Für eine erfolgreiche medizinische Behandlung ist ein intaktes Vertrauensverhältnis zwischen dem Arzt und seinen Patienten, zu dem nicht zuletzt auch die Wahrung der ärztlichen Schweigepflicht und des Datenschutzes gehört, eine unerlässliche Voraussetzung.

Diese Erkenntnis ist nicht überraschend, schließlich ist die ärztliche Schweigepflicht über 2500 Jahre alt. Bereits im alten Griechenland mussten die jungen Ärzte im Eid des Hippokrates schwören, die Geheimnisse ihrer Patienten zu wahren.

Es liegt also im wohlverstandenen Interesse nicht nur der Patienten, sondern auch der Ärzte, Arztgeheimnis und Datenschutz zu gewährleisten. Aus diesem Grunde habe ich die gemeinsame Aktion „Datenschutz in der Arztpraxis" initiiert, die sich an eine vergleichbare Aktion des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein anlehnt. Beteiligt sind an ihr

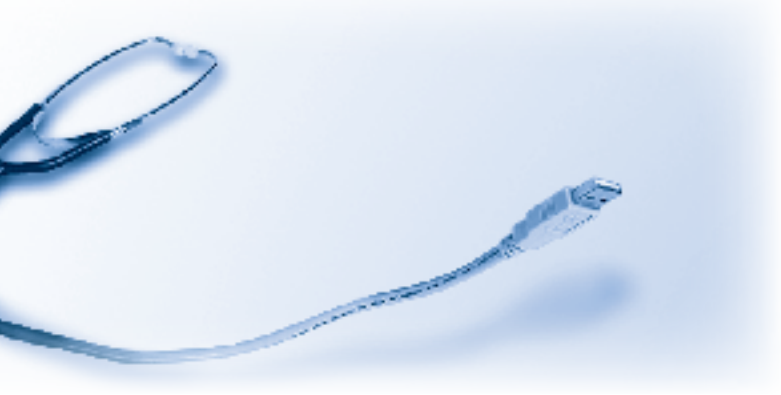
- die Ärzte-, die Zahnärzte- und die Psychotherapeutenkammer Niedersachsen,
- die Kassenärztliche Vereinigung Niedersachsen,
- das Niedersächsische Ministerium für Soziales, Frauen, Familie und Gesundheit,
- die Landesvereinigung für Gesundheit e. V.,
- der Berufsverband der Arzt-, Zahnarzt- und Tierarzthelferinnen (Landesverband Niedersachsen).

Ich bin sehr dankbar, dass es gelungen ist, die Aktion auf diese breite Basis zu stellen. Ärzte, Patientenvertreter, Datenschützer, nicht zuletzt auch Vertreterinnen der für die Umsetzung des Datenschutzes wichtigen Arzthelferinnen, haben ihre Vorstellungen in das Projekt eingebracht, das bisher zwei Umsetzungsstufen erlebt hat.

Was können die Ärzte tun?

Zunächst wurde den Ärzten, Zahnärzten und Psychotherapeuten ein in den Mitteilungsblättern der Kammern veröffentlichter Selbst-Check zur Verfügung gestellt, mit dem sie prüfen konnten, wie es in ihren Praxen um den Datenschutz bestellt ist. Angesprochen werden u. a.

- der Empfang (z. B. „Kann das Personal Telefongespräche führen, ohne dass zwangsläufig wartende Patientinnen und Patienten dadurch von Daten anderer Personen Kenntnis erlangen?"),



- der Behandlungsbereich („Sind Patientendaten in dem Behandlungszimmer gegen unbefugte Kenntnisnahme geschützt? Werden Unterlagen vorhergehender Behandlungen sofort in das Vorzimmer/an die Ablage zurückgegeben?“) und die
- EDV (etwa Fragen zur Vergabe und Verwaltung der Passwörter).

Für tiefergehende Informationen habe ich in meinem Internetangebot eine umfangreiche Arbeitshilfe bereitgestellt, in der die juristischen Grundlagen des Datenschutzes und der ärztlichen Schweigepflicht erläutert und praxisnahe Tipps für eine datenschutzgerechte Ausgestaltung der Arbeitsabläufe in der Arztpraxis gegeben werden.

Was können die Patienten tun?

Die Sicherstellung von Schweigepflicht und Datenschutz ist allerdings nicht nur Aufgabe des Arztes, auch die Patienten können und müssen ihren Teil dazu beitragen. So ist es nicht nur unhöflich gegenüber den anderen Patienten, den Arzt am Empfang „abzufangen“, um ohne lange Wartezeit die Untersuchungsergebnisse zu erfahren. Man zwingt ihn auch, vertrauliche Dinge vor Publikum zu erörtern. Um daher eine Sensibilisierung der Patienten zu erreichen, ist ein „Merkblatt für Patientinnen und Patienten“ mit entsprechenden Hinweisen entwickelt worden. Dieses Merkblatt ist in einer Auflage von 300.000 Exemplaren gedruckt worden, so dass es jeder Praxis in Niedersachsen in mehrfacher Anzahl zur Weitergabe an die Patientinnen und Patienten zur Verfügung gestellt werden konnte.

Wie geht es weiter?

Parallel zu den dargestellten Umsetzungsschritten habe ich umfangreiche Informationen zum Gesundheitsdatenschutz und zum Patientengeheimnis in mein Internetangebot eingestellt. Im Rahmen der Auswertung der bisherigen Aktionsschritte ist geplant, im nächsten Jahr auf entsprechende Anforderung hin Beratungsbesuche in ausgewählten Praxen zu machen. Außerdem möchte ich eine vergleichbare Aktion für die Verbesserung des Datenschutzes in Krankenhäusern starten.

Weiterer Handlungsbedarf besteht auch auf dem Gebiet der IT-Sicherheit in Arztpraxen. Gerade dort gibt es in vielen Bereichen noch große Unsicherheit, so dass von Seiten der Ärzteschaft die Bitte an mich herangetragen worden ist, bei der Erstellung eines entsprechenden Handbuchs – angefangen von der Feststellung des Schutzbedarfs für typische in den Arztpraxen eingesetzte Systemkonfigurationen bis hin zur Erstellung von konkreten Handlungskonzepten – mitzuwirken. Diesem Wunsch werde ich im Rahmen der mir zur Verfügung stehenden Kapazitäten gerne nachkommen.

Vertiefende Informationen zum Thema:

Selbst-Check, Merkblatt für Patienten und Arbeitshilfe stehen im Internetangebot des LfD Niedersachsen zur Verfügung:

www.lfd.niedersachsen.de
Themen/Gesundheit/Datenschutz in der Arztpraxis

Mehr zum Datenschutz in der Arztpraxis auch im Virtuellen Datenschutzbüro: **www.datenschutz.de**
Recht/Medizin/Arztpraxis

Zahlreiche weitere Informationen zum Datenschutz im Gesundheitswesen finden Sie unter:
www.datenschutz.de
Recht/Gesundheit.

„… und es hat zoom gemacht“ 10

… so titelte die Hannoversche Allgemeine Zeitung am 17.04.2004 und informierte ihre Leser über die bei einem hannoverschen Nahverkehrsunternehmen eingesetzte Videoüberwachung. Mit voyeuristischen Passagen wie: „Die Kamera stellt automatisch scharf. Man kann fast die Bartstoppeln des Mannes zählen.“ oder „… ist jetzt eine junge Frau zu sehen. Erst ihr Gesicht in Großaufnahme. Die Kamera tastet sich abwärts …“ wird der Leser gefesselt. Ob der Redakteur die technischen Möglichkeiten der Videoüberwachung auch so liebevoll ausgeschmückt hätte, wenn es um die im politischen Raum immer wieder geforderte flächendeckende Überwachung von Straßen und Plätzen durch die Polizei gegangen wäre?

Der Praxiseinsatz der Videoüberwachung im öffentlichen Nahverkehr in Hannover ist von meinen Mitarbeitern eingehend überprüft worden. Die Kontrolle gab im Wesentlichen keinen Anlass zu Beanstandungen, wohl auch deshalb, weil wir die vorbereitenden Arbeiten für dieses Vorhaben intensiv begleitet hatten. Andererseits ist Realität, dass Supermarktketten und Baumärkte für wenig Geld drahtlose Videofarbkameras, sogar mit eingebautem Mikrofon anbieten. Wen wundert es also, wenn sowohl Privatpersonen als auch Geschäftsleute sich aus diesem Angebot bedienen, ohne sich darüber Gedanken zu machen, ob eine Videoüberwachung überhaupt rechtlich zulässig ist.

Rechtliche Vorgaben für die Videoüberwachung

Der Gesetzgeber hat für die Videoüberwachung durch Privatpersonen oder Unternehmen in § 6b BDSG enge Grenzen gesetzt; diese gelten immer dann, wenn die Überwachung öffentlich zugängliche Bereiche erfasst. Ich habe daher in einem Faltblatt die wichtigsten Regeln für eine Videoüberwachung zusammengestellt:

- Videoüberwachung darf nur zu einem vor dem Einsatz konkret festgelegten und schriftlich festgehaltenen Zweck eingesetzt werden und muss dafür erforderlich sein. Allgemeine Formulierungen, wie z. B. „Abschreckung“, reichen dabei nicht aus. Der Schutz vor Diebstahl in Kaufhäusern kann ebenso eine Videoüberwachung rechtfertigen wie das Vermeiden des Besprayens bzw. Beschmierens einer Hausfassade, wenn andere Mittel keinen Erfolg versprechen. Auch die Aufklärung sonstiger Straftaten oder das Interesse, Verstöße vor Gericht beweisen zu können, kann ein rechtfertigender Zweck für eine Videoüberwachung sein.
- Die Rechte von Betroffenen dürfen nicht verletzt werden. Vor dem Einsatz müssen deren Interessen mit dem mit der Videoüberwachung verfolgten Zweck abgewogen werden. Ist z. B. das Interesse von Kunden oder Mitarbeitern, unbeobachtet agieren oder kommunizieren zu können, höher einzustufen, darf eine Videoüberwachung nicht stattfinden. Die schutzwürdi-

gen Interessen überwiegen regelmäßig dann, wenn sensitive Daten erhoben oder die Intimsphäre verletzt werden. Die Überwachung des Intimbereichs von Toiletten oder Umkleidekabinen ist daher nicht erlaubt.

- Auf die Videoüberwachung ist deutlich sichtbar hinzuweisen, z. B. durch ein gut erkennbares Hinweisschild am Eingang des überwachten Bereiches. Jeder soll so die Möglichkeit haben, sich der Überwachung zu entziehen. Aus dem Hinweisschild soll auch zu erkennen sein, an wen man sich bei Nachfragen wenden kann. Beim Einsatz von Videoüberwachung in Betrieben sind die Mitarbeiter über den Zweck und den Umfang der Videobeobachtung zu informieren, der Betriebsrat ist zu beteiligen.
- Eine heimliche Überwachung durch versteckte Kameras ist im Ausnahmefall als „ultima ratio" nur dann zulässig, wenn dies die einzige Möglichkeit darstellt, berechtigte und schützenswerte Interessen (z. B. Schutz des Eigentums bei wiederholten Diebstählen) zu wahren. Die befürchteten Rechtsverletzungen müssen durch konkrete Anhaltspunkte und Verdachtsmomente belegt sein. Eine nur vage Vermutung oder ein pauschaler Verdacht genügen nicht.
- Ist der Zweck erfüllt, muss die Videoüberwachung unverzüglich eingestellt werden.
- Sollen die Videobilder aufgezeichnet werden, ist hierfür erneut die Erforderlichkeit zu prüfen und eine Abwägung mit den Interessen der Betroffenen vorzunehmen. Es ist im Einzelnen festzulegen, wer zu welchem Zweck Zugang zu den gespeicherten Bilddaten hat und wie ihre verlässliche Löschung gewährleistet wird.

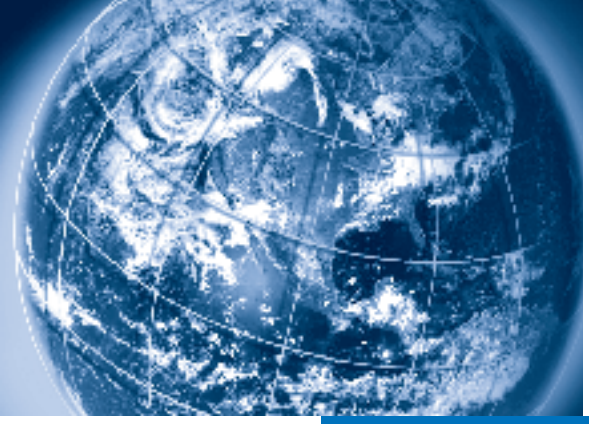
Soll bei einer Videoüberwachung auch der Ton mit einem Mikrofon aufgenommen werden, ist § 201 Strafgesetzbuch zu beachten, der das unbefugte Aufnehmen des nichtöffentlich gesprochenen Wortes eines anderen auf einen Tonträger oder das unbefugte Abhören mit einem Abhörgerät als Straftat verbietet.
Ich werde den Einsatz von Videoüberwachung im öffentlich zugänglichen Raum weiterhin kritisch begleiten und die Einhaltung der gesetzlichen Vorgaben einfordern.

Vertiefende Informationen zum Thema:

Faltblatt „Achtung Kamera!" beziehbar in der Geschäftsstelle des Landsbeauftragten für den Datenschutz Niedersachsen, ~~Brühlstraße 9, 30169 Hannover~~

www.lfd.niedersachsen.de (Themen/Videoüberwachung)

Prinzenstr. 5, 30159 Hannover



Die Welt AG – Datenaustausch ohne Grenzen? 11

Durch Internet und moderne Netzwerktechnologien können Daten aus Hannover heute genauso schnell in New York verarbeitet werden wie im Büro nebenan. Gleichzeitig tragen Globalisierung und Europäisierung dazu bei, dass mehr und mehr weltweite Konzernstrukturen und -verflechtungen entstehen. Immer öfter ist der mittelständische Traditionsbetrieb kein eigenständig arbeitendes Unternehmen mehr, sondern Teil eines weltweit operierenden Konzernverbundes.
Ist der Datenaustausch innerhalb des Konzerns problemlos möglich? Was ist zu beachten?

Stufe 1:
Erlaubnis für unternehmensübergreifende Datenverarbeitung im Konzern

Das Bundesdatenschutzgesetz (BDSG) kennt keinen Konzerndatenschutz. Diese oft übersehene Tatsache führt dazu, dass auch für die Übermittlung von personenbezogenen Daten eines Konzernunternehmens zu einem anderen angeschlossenen Unternehmen das grundsätzliche Verbot mit Erlaubnisvorbehalt gilt. Dieses Verbot richtet sich sowohl an ausschließlich im Inland als auch an global operierende Konzerne. Es kann überwunden werden, wenn der Betroffene in die Datenübermittlung einwilligt oder eine Erlaubnisnorm vorhanden ist.
Welche Erlaubnisnormen für einen konzerninternen Datentransfer herangezogen werden können, stellen die Datenschutzaufsichtsbehörden gerade in einer Arbeitsgruppe zusammen. Bis dahin ist eine Übermittlung von Daten immer im Einzelfall auf ihre Zulässigkeit zu überprüfen!
Ist diese erste Hürde überwunden, muss bei internationalen Datenübermittlungen in einem zweiten Schritt geprüft werden, ob auch die speziellen Anforderungen an eine Datenübermittlung ins Ausland erfüllt sind.

Stufe 2:
Die Erlaubnis für Datenübermittlung ins Ausland

Um Daten ins Ausland transferieren zu dürfen, muss man sich vergewissern, dass derjenige, dessen Daten übermittelt werden sollen, kein schutzwürdiges Interesse am Ausschluss dieser Übermittlung hat. Insbesondere muss ein angemessenes Datenschutzniveau beim Empfänger gewährleistet sein.
Die Beurteilung der Frage, ob ein schutzwürdiges Interesse des Betroffenen vorliegt und ob ein angemessenes Datenschutzniveau beim Empfänger vorhanden ist, hat das übermittelnde Unternehmen in eigener Verantwortung vorzunehmen!

Der Sitz des Datenempfängers

Völlig unproblematisch ist der Transfer in Länder und Institutionen, die der Europäischen Union (EU) oder dem Europäischen Wirtschaftsraum (Norwegen, Liechtenstein, Island) angehören, weil hier durch die verpflichtende Wirkung der EU-Datenschutz-Richtlinie ein einheitlicher Rahmen für den Datenschutz vorgegeben ist.
Ein angemessenes Datenschutzniveau kann darüber hinaus für einzelne Länder auch von der Kommission anerkannt werden. Eine solche Anerkennung ist

erfolgt bei Argentinien, der Schweiz, Ungarn, Guernsey und der Isle of Man und einigen Bereichen Kanadas. Die Anerkennung eines angemessenen Datenschutzniveaus in den USA ist von einem Beitritt des Daten empfangenden Unternehmens zum sogenannten Safe Harbour-Abkommen abhängig. Ebenso hat die EU festgestellt, dass aufgrund eines ausgehandelten Abkommens auch bei der Übermittlung von Flugpassagierdaten in die USA ein angemessenes Datenschutzniveau angenommen werden kann. Diese Feststellung ist jedoch aus meiner Sicht nicht haltbar und wird auch auf politischer Ebene weiter diskutiert.

Standardvertragsklauseln

Eine gute Alternative bieten die von der EU-Kommission erarbeiteten Standardvertragsklauseln. Werden diese in einem Vertrag zwischen übermittelndem und empfangendem (Konzern-) Unternehmen eingesetzt, kann ein angemessenes Datenschutzniveau beim Empfänger angenommen werden.
Ich empfehle den von mir beratenen Firmen, möglichst auf diese Variante zurückzugreifen, da der hinter den Standardvertragsklauseln liegende Text einigermaßen übersichtlich, kompakt und verständlich die notwendigen Anforderungen an eine Datenübermittlung regelt.

Weitere Faktoren

Anderenfalls muss das Unternehmen eine individuelle Bewertung zur Angemessenheit des Datenschutzniveaus durchführen. Hierbei können folgende Faktoren Berücksichtigung finden:

- die Art der übermittelten Daten,
- die Zweckbestimmung,
- die Dauer der geplanten Verarbeitung,
- das Herkunfts- und das Endbestimmungsland,
- die für den betreffenden Empfänger geltenden Rechtsnormen sowie
- die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen.

Kommt das übermittelnde Unternehmen zu dem Schluss, dass bei einer Bewertung aller denkbaren Faktoren eine empfangende Stelle ein im Verhältnis zur EU-Datenschutzrichtlinie und zum BDSG angemessenes Datenschutzniveau hat, dürfen die personenbezogenen Daten übermittelt werden.

Die Unternehmensregelungen (Codes of Conduct)

Eine besondere Bedeutung kommt den internen Unternehmensregelungen – oft auch „Codes of Conduct“ genannt – zu. Diese Regelungen können dann ein angemessenes Datenschutzniveau begründen, wenn sie von ihrem Inhalt her die datenschutzrechtlichen Mindeststandards des BDSG beinhalten. Die Codes of Conduct sollten sich an den Standardvertragsklauseln orientieren, insbesondere im Hinblick auf die Drittbegünstigtenklausel und die Haftungsregeln.

Inhaltliche Abweichungen sind dann unschädlich, wenn sie durch sonstige verbindliche Regelungen oder organisatorische Maßnahmen hinreichend kompensiert werden.

Ausnahmen

Darüber hinaus hat der Gesetzgeber in § 4c BDSG zahlreiche Ausnahmetatbestände für das sonst geforderte angemessene Datenschutzniveau vorgesehen. Liegt ein Ausnahmetatbestand vor, gibt es keine Einwände gegen die Übermittlung.

Dies ist zum Beispiel dann der Fall, wenn der Betroffene in den Datentransfer eingewilligt hat oder wenn zur Erfüllung eines Vertrages die Übermittlung von Daten ins Ausland notwendig ist.

Insbesondere die letztgenannte Möglichkeit wird aber oft falsch ausgelegt; so greift diese Ausnahme in der Regel nicht, wenn im Rahmen eines vertraglichen Arbeitsverhältnisses Daten zur Konzernzentrale im Ausland übermittelt werden sollen, da zur Erfüllung des Vertrages – nämlich der Abwicklung eines Arbeitsverhältnisses – die Übermittlung der Daten nicht zwingend erforderlich ist.

Letzte Möglichkeit: Die Aufsichtsbehörde

Wenn auf Grund der dargestellten Möglichkeiten der Transfer der Daten noch nicht erlaubt ist, kann die Aufsichtsbehörde in Einzelfällen eine Genehmigung erteilen, die aber im Ergebnis zu keinen gravierenden Abstrichen vom europäischen Datenschutzniveau führen darf.

Mein Beratungsangebot

Damit der Datenschutz nicht zu einem Hindernis für den internationalen Handel und das weltumspannende Wirtschaften wird, stehen meine Mitarbeiterinnen und Mitarbeiter zusammen mit dem Innenministerium allen niedersächsischen Unternehmen gerne für eine Beratung darüber zur Verfügung, wie die bestehenden Regelungen ergebnisorientiert umgesetzt werden können.

Vertiefende Informationen zum Thema:

Internet:
www.lfd.niedersachsen.de
– Themen, Internationaler Datenverkehr

Recht: §§ 4b und 4c BDSG, aber auch Ergänzung in § 3 Abs. 8 BDSG.
Artikel 25 und 26 der Richtlinie 95/46/EG.

Safe Harbour:
www.export.gov/safeharbor/

EU-Kommission, GD Binnenmarkt – Datenschutz:
www.europa.eu.int/comm/internal_market/privacy/index_de.htm
Standardvertragsklauseln, Angemessenheit des Schutzes personenbezogener Daten in Drittländern, Safe Harbour.

Kundendaten 12

Nie waren sie so wertvoll wie heute

Unmittelbarer und möglichst enger Kundenbezug sowie Direktwerbung sind nach wie vor die aktuellen Strategien des Marketing. Kein Wunder, dass daher die Jagd nach möglichst aussagefähigen Informationen über Kaufgewohnheiten, Produktvorlieben und Verbrauchsverhalten des Einzelnen in vollem Gange ist und immer neue Wege entwickelt werden, um an diese Informationen heranzukommen. Neben der „klassischen" Erhebung im Zusammenhang mit dem einzelnen Kaufvorgang, bei dem nur die zur Abwicklung des konkreten Warenaustausches notwendigen Daten erhoben werden, werden kundenbezogene Informationen immer häufiger auch außerhalb konkreter Kaufvorgänge, etwa über Preisausschreiben, Werbeaktionen oder Befragungen, gesammelt. Besondere Bedeutung haben auch Kunden- oder Rabattkarten gewonnen, die häufig auch nicht nur firmenbezogen eingesetzt, sondern in übergreifenden Verbünden ausgegeben und ausgewertet werden.

Welche Regeln müssen beachtet werden?

Um hier sowohl für Kunden als auch für Firmen Klarheit über die rechtlichen Rahmenbedingungen zu schaffen, habe ich in Abstimmung mit dem Niedersächsischen Einzelhandelsverband die wichtigsten Regeln für das Erheben und Auswerten von Kundendaten zusammengestellt und sowohl über mein Internetangebot als auch durch gezielte Beratungen verbreitet.

Die wichtigsten Regeln sind die folgenden:

- Bei Abschluss eines Kauf- oder Dienstleistungsvertrages dürfen nur Daten abgefragt werden, die für die Erfüllung des Vertrages erforderlich sind. Dies hängt entscheidend von den vereinbarten Rechten und Pflichten sowie den Rahmenbedingungen (Lieferung, Ratenzahlung usw.) ab.
- Sollen die abgefragten und gespeicherten Daten für andere Zwecke genutzt werden (z. B. Werbung, Kontaktpflege), sind die Kunden darauf hinzuweisen.
- Die Nutzung von Daten für Werbezwecke ist zulässig, wenn eine Einwilligung dafür vorliegt. Diese Einwilligung muss aber bewusst und freiwillig erfolgt sein, schriftlich vorliegen und sich ausdrücklich auf die Verwendung der Daten zum Zwecke der Werbung beziehen. Die Einwilligung ist der freien Disposition des Kunden unterworfen und ein Widerspruch gegen eine Nutzung zu Werbezwecken darf keine Auswirkungen auf das Grundverhältnis haben.

- Die Einwilligung ist besonders hervorzuheben und darf nicht in den Allgemeinen Geschäftsbedingungen versteckt werden. Wird diese Einwilligung elektronisch, etwa über eine Internetseite eingeholt, muss dafür eine aktive und bewusste Handlung, z. B. über das Anklicken eines Buttons, erfolgen.
- Liegt eine Einwilligung nicht vor, so ist die Nutzung der Daten für Werbezwecke nur zulässig, wenn
  – die Daten allgemein zugänglich sind, oder
  – das Unternehmen, das die Daten nutzen will, sieveröffentlichen dürfte, oder
  – es sich um listenmäßig zusammengefasste Daten über Angehörige einer Personengruppe handelt.
- In diesen Fällen darf kein Grund zu der Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss einer solchen Nutzung hat.
- Werden Kundendaten zulässigerweise listenmäßig an andere Unternehmen weitergegeben, so empfehle ich, die Kunden auf eine beabsichtigte Weitergabe an Dritte zu Werbezwecken hinzuweisen.
- Allerdings ist nicht jede Art der Werbung unter Nutzung personenbezogener Daten erlaubt. Es ist z. B. zulässig, aus dem Internet eMail-Adressen potentieller Kunden zu gewinnen und zu speichern. Diese Adressen dürfen aber nicht für das Versenden von Werbe-eMails genutzt werden, weil das nur mit der vorherigen Einwilligung der Empfänger gestattet ist. Dies gilt ebenso auch bei Werbung über SMS, Fax oder Telefon. Widerspricht ein Kunde der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung, ist eine solche Nutzung oder Übermittlung unzulässig. In diesem Fall muss ein Eintrag in einer Sperrdatei erfolgen, die bei künftigen Werbeaktionen abgeglichen wird.
- Wird jemand speziell zum Zwecke der Werbung angesprochen, ist er über dieses Widerspruchsrecht zu informieren. Es ist ihm außerdem mitzuteilen, welche Stelle oder Unternehmen die Daten erhebt, verarbeitet oder nutzt.
- Werden die genutzten personenbezogenen Daten bei einer Stelle gespeichert, die dem Betroffenen nicht bekannt ist, muss sichergestellt sein, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann.
- Daten zum Kauf- oder Zahlungsverhalten dürfen nur mit vorheriger Einwilligung weitergegeben oder genutzt werden. Diese ist nur wirksam, wenn der Kunde dabei über den Zweck der Datenerhebung, -verarbeitung und -nutzung unterrichtet wurde. Außerdem muss darauf hingewiesen worden sein, dass die Einwilligung freiwillig ist und zu jeder Zeit widerrufen werden kann.
- Daten, deren Kenntnis für die Erfüllung des Vertragszwecks nicht mehr erforderlich ist, sind zu löschen. Unterliegen die Daten einer gesetzlichen Aufbewahrungsfrist, sind sie nach Wegfall der Erforderlichkeit zu sperren.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de/
Service-Angebote,
Fragen auf Antworten

www.datenschutzzentrum.de/
wirtschaft/
Kundenbindungssysteme.pdf

13 Scoringverfahren

Der Mensch als Zahl?

Die Bewertung von persönlichen Leistungen mittels einer Zahl (Note) ist jedem aus der Schule bekannt. Bei so genannten Scoringverfahren bewerten Unternehmen ihre Kunden. Dies geschieht durch mathematisch-statistische Verfahren, in denen ein Datenbestand insgesamt anonymisiert hinsichtlich gewünschter Wahrscheinlichkeitsaussagen analysiert wird (z. B. Wer verursacht überdurchschnittlich viele Verkehrsunfälle?). Die in Zahlen ausgedrückten Ergebnisse beziehen sich zunächst auf Einzelmerkmale (z. B. Alter: 18–25jährige = hohe Unfallrate = niedriger Scorewert). Die Werte mehrerer Einzelmerkmale (etwa Einkommen, Alter, Beruf, Geschlecht, Familienstand) können in ihrer Summe einen Gesamtscorewert bilden. Der Gesamtscorewert eines Kunden setzt sich aus den Einzelwerten zusammen, die für die jeweils zu ihm passende Vergleichsgruppe ermittelt wurden.

Die Ziele der Scoringverfahren sind unterschiedlich. Häufig geht es den Unternehmen um die Einschätzung der finanziellen Leistungsfähigkeit ihrer Kunden und ihrer zukünftigen Zahlungsbereitschaft. Das Ergebnis der Bewertung, der Scorewert, wird von den Unternehmen etwa bei der Vergabe von Krediten oder beim Abschluss von Versicherungsverträgen als Entscheidungshilfe herangezogen. Er wird als ein Wahrscheinlichkeitsindex etwa über mögliche Forderungsausfälle bei Antragstellern oder Kunden betrachtet.

Werden wirklich nur statistische Daten verarbeitet?

Scoringverfahren gewinnen in Unternehmen zunehmend an Bedeutung. Es geht dabei um die Kategorisierung und Klassifizierung der vorhandenen Daten. Dies soll den Unternehmen ermöglichen, ihre Aktivitäten zielorientiert auszurichten und ihre Ressourcen effizienter einzusetzen.

Aber ist das Scoring wirklich nur eine datenschutzrechtlich unproblematische Verarbeitung anonymisierter statistischer Daten? Unterschieden werden muss die statistische Analyse und Bewertung anonymer Vergleichsgruppen von der Zuordnung eines aus diesem Vorgang resultierendem Scorewertes zu einer natürlichen Person. Die Einordnung eines Kunden in eine bestimmte Vergleichsgruppe und die Übernahme des dieser Vergleichsgruppe zugeteilten Einzelwertes im Rahmen eines Scorings ist aus meiner Sicht ein Bearbeitungsvorgang mit Personenbezug, für den daher zu fragen ist, inwieweit er die rechtlichen Voraussetzungen erfüllen muss, die auch sonst für die Verarbeitung personenbezogener Daten gelten. Von Seiten der Wirtschaft wird vielfach die Auffassung vertreten, es gehe beim Scoring allein um die Verarbeitung anonymisierter statistischer Daten ohne Personenbezug. Das ist richtig, soweit es sich auf die Er-

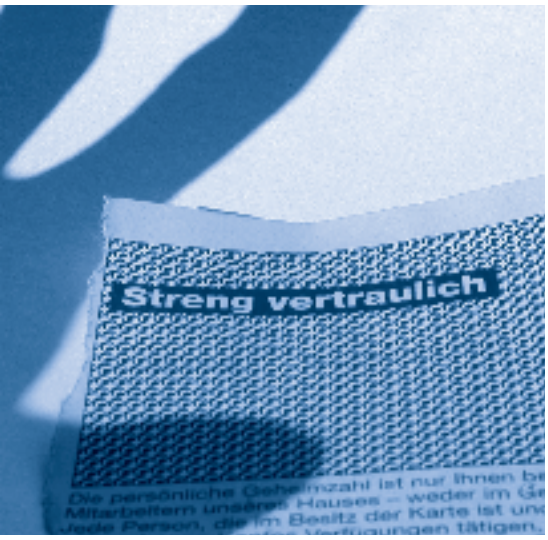
mittlung der statistischen Grundlagen bezieht. Diese Meinung übersieht jedoch, dass mit der Zuordnung eines Scorewertes zu einer Person über diese konkrete Person in einer konkreten Situation eine Aussage über konkrete Eigenschaften getroffen wird. Ein Scorewert ohne Bezug zu einer bestimmten Person wäre für den Anwender wertlos, da er als Entscheidungshilfe nicht tauglich wäre. Die Diskussion muss in diesem Punkt weiter geführt und intensiviert werden.

Kreditentscheidung nach Tabelle

Insbesondere das Kreditscoring ist Gegenstand andauernder Diskussionen im Berichtszeitraum gewesen. Dies ist unter anderem auf eine Vereinbarung der Zentralbanken und Finanzaufsichtbehörden zurückzuführen (sog. Basel II-Abkommen). Danach bemisst sich das Kreditvolumen von Banken ab 2006 an dem Ausfallrisiko der ausgegebenen Kredite. Je geringer das Ausfallrisiko eines ausgegebenen Kredites für eine Bank ist, desto geringer ist auch das von ihr dafür vorzuhaltende Eigenkapitel. Die Bank kann also bei geringen Ausfallrisiken im Ergebnis mehr Kredite ausgeben. Die Entscheidung über Privatkredite und vor allem die Kosten für Kreditaufnahmen werden sich zukünftig stärker als bisher an den Ergebnissen von Scoringverfahren orientieren.

Weitere Anwendungsbereiche

Neben dem Kreditscoring sind unter anderem auch Werbe-, Verhaltens- oder Beitreibungsscoringverfahren (letztere im Inkassobereich) denkbar. Werden etwa Informationen über die durchschnittliche Zahlungskraft von bestimmten Stadtteilen oder Ortschaften mit Adressinformationen von Kunden verknüpft, können so gezielt zahlungskräftigere Kunden beworben werden.
Bei den gesetzlichen Krankenkassen bestehen dem Vernehmen nach Überlegungen, Scoringverfahren einzusetzen, um diejenigen Kunden zu ermitteln, deren Mitgliedschaft von besonderem Wert ist und bei denen Bemühungen zur Pflege der Beziehung besonders lohnend erscheinen.



Interne und externe Scorewerte

Scorewerte können in Unternehmen auf zwei Wegen zum Einsatz kommen:

1. Das Unternehmen legt selbst Parameter fest, an Hand derer die im Unternehmen vorhandenen Kundendaten bewertet und kategorisiert werden sollen.
2. Das Unternehmen übernimmt Scorewerte, die ein anderes Unternehmen (etwa die Schufa) ermittelt hat.

Datenschutzrechtliche Anforderungen an Scoringverfahren

Über den geplanten Einsatz von internen Scoringverfahren und Verwendung von extern ermittelten Scorewerten habe ich mit Banken, Versicherungen und Krankenkassen Gespräche geführt.

Im derzeitigen Stadium der Diskussion besteht das Hauptproblem in der Intransparenz der Scoringverfahren. Eine adäquate datenschutzrechtliche Bewertung setzt die genaue Kenntnis darüber voraus, welche Daten in das Verfahren einfließen, woher diese Daten stammen und welche Konsequenzen das Scoring für die Entscheidungsprozesse der Unternehmen hat. Die Betroffenen selbst wissen in aller Regel gar nicht, dass für sie ein Scorewert ermittelt und gespeichert wurde. Unabhängig davon wäre für sie aber auch nicht nachvollziehbar, wie der sie betreffende Scorewert zu Stande kommt. Auch erhalten sie keine Gelegenheit, nachzuweisen, dass die der statistischen Vergleichsgruppe zugeordnete Bewertung (etwa: Kraftfahrer im Alter von 18 bis 25 Jahren verursachen überdurchschnittlich viele Verkehrsunfälle) auf sie nicht zutrifft. Die Durchsetzung der Betroffenenrechte (Auskunft, Berichtigung, Löschung, Sperrung) sind dementsprechend erschwert.

Weiter besteht die Forderung, dass Persönlichkeitsmerkmale und Daten, deren Bewertung diskriminierenden Charakter haben kann, dazu zählen insbesondere sensitive Daten (z. B. Gesundheit, ethnische Herkunft, politische Meinung, Religionszugehörigkeit, Sexualleben), nicht in ein Scoring-Verfahren einbezogen werden dürfen.

Problematisch an Scoringverfahren ist darüber hinaus die Pauschalität der Bewertungen, die zwangsläufig mit der Zuordnung des einzelnen Kunden zu statistischen Vergleichsgruppen verbunden ist.

Schließlich muss auch geprüft werden, inwieweit der Einsatz von Scoringverfahren gegen das Verbot automatisierter Einzelentscheidungen in § 6a BDSG verstößt.

Die datenschutzrechtliche Bewertung von Scoringverfahren der gesetzlichen Krankenkassen bemisst sich nach den, gegenüber dem BDSG strengeren, Vorschriften des SGB V und X. Die Zulässigkeit entsprechender Scoringverfahren bei den Krankenkassen sowie die datenschutzrechtlichen Rahmenbedingungen für den Einsatz von Scoringverfahren in Unternehmen müssen noch weiter geprüft und mit den entsprechenden Organisationen und Verbänden diskutiert werden.

Vertiefende Informationen zum Thema:

www.datenschutz.de Suche zu „Scoring"

www.bfd.bund.de Datenschutz von A–Z: Stichwort Schufa;
Bürger fragen: Auskunft über eigenen Scorewert

Petri, Sind Scorewerte rechtswidrig?, in: DuD 2003, S. 631–636

RFID und Datenschutz 14

Die Technik der Radio Frequency Identification (RFID) ist nicht neu. Doch durch die fortschreitende Miniaturisierung und die größere Leistungsfähigkeit der Funkchips sehen Industrie und Handel ebenso wie Sicherheitsbehörden und Verwaltungen ganz neue Einsatzmöglichkeiten. Eine datenschutzgerechte Ausgestaltung dieser neuen Möglichkeiten soll der ungezügelten Datensammelei und dem Missbrauch der Datensammlungen vorbeugen und einen verantwortungsvollen Umgang mit RFID ermöglichen.

Radio-Frequency-Identification (RFID) 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.

Einsatzfelder und Funktion

RFID wird bereits heute für eine Reihe unterschiedlicher Zwecke aus dem Bereich der Warenlogistik, der Produktionsautomation sowie im Bereich der Warenauthentisierung eingesetzt. Im Einzelhandelsbereich waren RFID-Anwendungen in der Vergangenheit auf den Einsatz als Diebstahlsicherung begrenzt. Bei ordnungsgemäß bezahlten Waren kam der Endverbraucher bislang mit RFID-basierender Technik praktisch nicht in Berührung. Künftig jedoch soll nach den Vorstellungen großer Handelsunternehmen auch in diesem Bereich RFID-Technik vermehrt zur Warenkennzeichnung zum Einsatz kommen und den bekannten EAN-Code verdrängen. Auch Funktionserweiterungen für Kundenbindungssysteme werden in diesem Zusammenhang bereits diskutiert. Eine testweise Einführung von RFID-Systemen im Metro Future Store hatte zu einer starken Verunsicherung der Kunden geführt, da diese unzureichend informiert worden waren. Auch über den Einsatz von RFID-Technologie bei Geldscheinen, Personalpapieren und Zutrittsberechtigungen wird derzeit intensiv diskutiert. Ein Beispiel hierfür sind die Eintrittskarten zur Fussball-WM 2006 oder die Geldscheine der Europäischen Zentralbank, die unter Anwendung von RFID-Technik gesichert werden sollen.

Daten(un)sicherheit

Neben Vorteilen in den genannten Einsatzgebieten birgt diese Technologie eine Reihe von Gefahren für das Recht auf informationelle Selbstbestimmung des Einzelnen. Insbesondere durch die Zuordnung von eindeutig gekennzeichneten Waren, Geräten und Gebrauchsgegenständen zu ihrem jeweiligen Besitzer besteht die Möglichkeit, Nutzungs- oder Bewegungsprofile zu erzeugen, ohne dass der Betroffene davon Kenntnis erlangt oder den Erhebungsvorgang beeinflussen kann. Auch die unbemerkte, automatisierte Einschätzung der Wirtschaftskraft einzelner Verbraucher wäre nach Einführung dieser Technologie bei der Kennzeichnung von Geldscheinen durchaus vorstellbar. Eine derartige Entwicklung wäre ein weiterer Schritt in Richtung „gläsener Verbraucher“, ergänzt durch die „gläserne Geldbörse“.

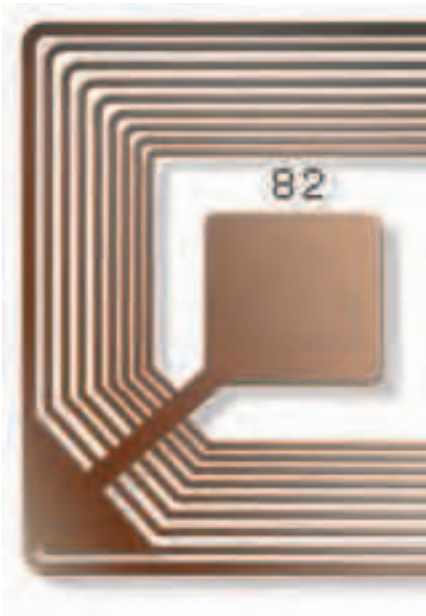
Vorbeugen und Aufklären

Um derartigen Entwicklungen frühzeitig entgegenzutreten, habe ich die folgenden Forderungen an die Hersteller von RFID-Systemen und die Nutzer dieser Technik zur Kennzeichnung von Waren und Gebrauchsgegenständen aufgestellt:

- Die Betroffenen sind umfassend über Einsatz und Verwendungszweck zu informieren,
- die RFID-Systeme sind so weiter zu entwickeln, dass RFID-Chips ohne Verarbeitungsfunktion eine Löschung aller Daten durch die Betroffenen ermöglichen,
- im Endkundengeschäft sind geeignete Geräte für eine Löschung der auf dem RFID-Chip gespeicherten Daten bei Verlassen der Verkaufsräume kostenfrei bereitzuhalten,
- für RFID-Systeme mit Verarbeitungsfunktion ist sicherzustellen, dass eine Kommunikation zwischen Lesegerät und RFID-Chip nur mit Kenntnis und Einwilligung des Betroffenen erfolgt,
- die Vertraulichkeit der Kommunikation sowie der auf dem RFID-Chip gespeicherten Daten ist durch geeignete technische Maßnahmen verlässlich sicherzustellen,
- Betroffene müssen kostenfrei Gelegenheit erhalten, sich Kenntnis über die auf einem RFID-Chip gespeicherten Informationen zu verschaffen,
- es sind RFID-Systeme anzubieten, die nicht über eine eindeutige Kennzeichnung identifizierbar sind.

Künftige Entwicklung

Nur durch den transparenten Einsatz und eine für die Betroffenen nachvollziehbare technische Ausgestaltung der RFID-Technologie können auch künftig die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit sichergestellt werden. Auch beim Einsatz von miniaturisierten und in Produkte eingebetteten IT-Systemen muss das Recht auf informationelle Selbstbestimmung in vollem Umfang gewährleistet bleiben.



Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de
> Service-Angebote > Technische Hilfen > RFID

http://de.wikipedia.org/wiki/RFID
Ausführliche Darstellung der Thematik RFID mit zahlreichen Links zu den unterschiedlichsten Anbietern weiterführender Informationen

Biometrie und Datenschutz 15

Nach den Terroranschlägen vom 11. September 2001 haben biometrische Verfahren eine ungeheure Aufwertung erfahren. Mit der geplanten Speicherung biometrischer Merkmale von Fingern, Händen oder Gesicht in Personalpapieren erhält die Diskussion um notwendige Sicherheitsmaßnahmen, Datenmissbrauch und zentrale Datensammlungen neuen Zündstoff.

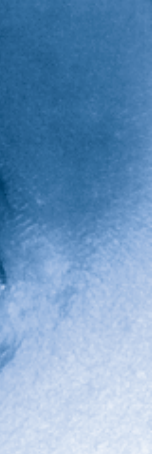
Die Biometrie ist die Wissenschaft der Körpermessung am Lebewesen. Biometrische Verfahren nutzen physische (Fingerabdruck, Gesicht, Muster der Iris) oder verhaltensbedingte Merkmale (Schreibverhalten, Lippenbewegung, Stimme) zur Identifikation einer Person. Die meisten biometrischen Merkmale verändern sich schon auf Grund des natürlichen Alterungsprozesses der betreffenden Person im Laufe der Zeit und bieten daher keine absolute Erkennungssicherheit über längere Zeiträume hinweg.

Bei der Anwendung der Biometrie wird unterschieden zwischen der Personenidentifikation und der Personenverifikation. Während die Identifikation die Erkennung einer ganz bestimmten Person aus einer größeren Gruppe von Menschen zum Ziel hat, wird bei der Verifikation lediglich die Übereinstimmung vorgegebener Merkmale mit den Merkmalen geprüft, die eine anwesende Person präsentiert. Bekannteste Anwendungsfälle hierfür sind die Zugangssicherungen von Rechenzentren oder anderen sensitiven Bereichen, die der Kinobesucher der 80er-Jahre schon in den James-Bond-Filmen bestaunen konnte. Die Identifikation hingegen wird z. B. für die automatisierte Erkennung gesuchter Personen eingesetzt. 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.

Mögliche Gefährdungen durch den Einsatz der Biometrie …

Systembedingt lassen sich aus Rohdaten der Biometrie über den eigentlichen Verwendungszweck hinaus weitere Rückschlüsse auf persönliche Merkmale und Eigenschaften ziehen. Zum Beispiel kann aus dem Augenhintergrund auf Krankheiten wie Diabetes oder Bluthochdruck geschlossen werden. Daher habe ich mich frühzeitig dafür eingesetzt, dass beim Einsatz von Biometrie ausschließlich auf mathematische Komprimate zurückgegriffen werden darf, um den Zugang zu derartigen überschießenden Informationen aus Rohdaten und einen eventuellen Missbrauch zu vermeiden.

Die datenschutzrechtliche Bewertung der Biometrie hängt auch in starkem Umfang vom Einsatzzweck und von der technischen Ausgestaltung des Verfahrens ab. Datenschutzprobleme entfallen weitgehend, wenn auf eine zentrale Spei-



cherung verzichtet wird und die Betroffenen das Speichermedium, zum Beispiel eine Chipkarte, selbst verwalten. Sollten Referenzdaten hingegen zentral gespeichert werden, müssen die Zugriffsberechtigungen eindeutig festgelegt und verlässliche Sicherungsmechanismen nach dem aktuellen Stand der Technik (z. B. durch sichere Verschlüsselung) definiert und umgesetzt werden. Beim Einsatz biometrischer Auswertungsprogramme besteht außerdem die Gefahr, dass eine automatisierte Identifikation ohne Kenntnis der Betroffenen durchgeführt wird und dass daraus Bewegungs- und Verhaltensprofile gebildet werden. Diese Gefahr besteht insbesondere bei der Beobachtung öffentlicher oder privater Plätze unter Nutzung von Video-Technik, die mit einem biometrischen Erkennungssystem gekoppelt ist.

… kann durch geeignete Gestaltung der Verfahren wirksam begegnet werden

Um sicherzustellen, dass der Einsatz biometrischer Verfahren in Niedersachsen datenschutzgerecht erfolgt, begleiten wir Pilotverfahren in verschiedenen Bereichen und erarbeiten gemeinsam mit den Nutzern aus Verwaltung und Wirtschaft datenschutzfreundliche Konzepte für den Einsatz und die technische Ausgestaltung der Verfahren. Im Rahmen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begleiten wir intensiv die Beratungen über die beabsichtigte Einführung biometrischer Merkmale in Ausweisen und Pässen. Der Arbeitskreis Technik der Konferenz hat in einem Positionspapier Anforderungen für einen datenschutzgerechten Einsatz biometrischer Verfahren formuliert, die Grundlage für unsere Beratungsarbeit sind.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de
> Themen > Biometrie
> Themen > Sicherungstechnik

http://de.wikipedia.org/wiki/Biometrie
Umfassende und verständliche Informationen zum Themenkomplex Biometrie mit Verweisen auf eine ganze Reihe interessanter Dokumente und Grundlagendarstellungen

Sichere Funknetzwerke 16

Die Risiken für die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der im Netzwerk übertragenen Daten werden von vielen Betreibern derartiger Technik unterschätzt oder gar nicht erst wahrgenommen. Dadurch werden Endgeräte und sogar ganze Netzwerk-Infrastrukturen über das Einfallstor „WLAN" angreifbar.

Der Einsatz von Wireless Local Area Networks (WLAN) und Bluetooth-Technologien in Unternehmen, Verwaltungen und im Privatbereich verzeichnet rasante Zuwachsraten. Gleichzeitig steigt damit die Zahl der ungesicherten Funknetze und der Missbrauchsversuche. Für einen vergleichsweise geringen Preis werden Geräte heute bei jedem Technik-Discounter angeboten oder von Telekommunikationsanbietern bei Vertragsabschluss kostenlos dazugegeben. Und genauso leicht wie die Anschaffung ist vermeintlich auch die Konfiguration und Absicherung der Funknetze.

WLAN und Bluetooth

Grundsätzlich ist zwischen Funknetzen auf der Basis der Standards IEEE 802.11x (Wireless LAN) und IEEE 802.15.1 (Bluetooth) zu unterscheiden. Während Bluetooth für den Aufbau drahtloser Ad-hoc-Verbindungen zwischen unterschiedlichen Endgeräten (Handy, PDA, Drucker, etc.) und für kurze Distanzen gedacht ist, ersetzen WLAN-Verbindungen reguläre kabelgebundene Netzwerke oder ergänzen diese funktional. Dabei reichen die Sendeleistungen der Sendestationen (Access Points) bis zu mehreren hundert Metern.

Betriebsmodi

Funknetzwerke können in verschiedener Form und Ausprägung betrieben werden. Neben Ad-Hoc Verbindungen zweier WLAN- oder Bluetooth-Geräte werden vor allem WLAN-Netze im Infrastruktur-Modus aufgebaut, bei denen ein oder mehrere Access Points die Vermittlung der Datenpakete zwischen den WLAN-Geräten übernehmen. Sind die Access Points mit dem kabelgebundenen Netzwerk des Betreibers verbunden, können darüber zusätzliche Dienste (z. B. Internet, Datenbankserver, E-Mail) genutzt werden. Aus den verschiedenen Betriebsarten ergeben sich unterschiedliche Angriffsmöglichkeiten. Überwiegend richten sich die Angriffe gegen die Access Points, da sie den Zugangspunkt zum gesamten kabellosen und ggf. auch zum kabelgebundenen Netzwerk ermöglichen. Aber auch die drahtlosen Endgeräte selbst können angegriffen werden.

Sicherheitsschwächen

Mit der Einführung von WLAN wurden von den Herstellern auch Sicherheitsstandards entwickelt, die die Kommunikation zwischen drahtlosen Geräten und den Access Points schützen sollen. Inzwischen sind viele der Sicherheitsmechanismen kompromittiert und lassen sich mit frei verfügbaren Programmen brechen oder aushebeln. Neben den heute bekannten technischen Schwächen der angebotenen Absicherungsmethoden sind gerade im Privatbereich und in kleinen Unternehmen und Verwaltungseinheiten vor allem die mangelnden Kenntnisse der Betreiber sowie die vermeintlich einfach zu handhabende Technik die Ursachen für unzureichend oder gänzlich ungesicherte Funknetze.

Sicherungsmaßnahmen

Art und Umfang der getroffenen Sicherungsmaßnahmen entscheiden über die tatsächliche Sicherheit des Funknetzes. So kann zumeist mit einfachen Sicherungsmaßnahmen bereits ein ungezielter Angriff (z. B. durch Wardriving) abgewehrt werden. Für die Abwehr möglicher zielgerichteter Angriff müssen darüber hinaus zusätzliche technische und organisatorische Maßnahmen ergriffen werden.

Risikoeinschätzung …

Um die Risiken des Einsatzes eines WLAN richtig einschätzen zu können, ist von Verwaltung und Unternehmen eine Vorabkontrolle gem. § 7 Abs. 3 NDSG bzw. § 4d Abs. 5 BDSG durchzuführen. In der Vorabkontrolle sollen Angriffspunkte im Netzwerk, die Risiken des Betriebes und deren Eintrittswahrscheinlichkeiten bewertet und daraufhin die geeigneten technischen und organisatorischen Maßnahmen getroffen werden.

… und Maßnahmen

Für die niedersächsische Landesverwaltung habe ich zwei Muster-Vorabkontrollen sowie ein Informationsblatt mit Anmerkungen für den praktischen Einsatz erarbeitet, die unterschiedliche Szenarien für den Betrieb zu Grunde legen. Wesentliche Grundschutzmaßnahmen sind:

- Ändern des Standard Identifikationsnames (SSID) des Access Points und soweit möglich deaktivieren der SSID-Rundsendung,
- statische IP-Adressen und Adressfilterung im WLAN verwenden,
- Filter für die Hardware-Adressen der Funknetzwerkkarten (MAC-Adressen) einrichten,
- richtlinienkonformes Kennwort für das Admin-Konto der Access Points vergeben,
- geeignete Verschlüsselungsmechanismen einrichten (möglichst neuester Verschlüsselungsstandard),
- zentralen Aufstellungsort für die Access Points wählen und die Sendeleistung begrenzen,
- Access Point deaktivieren, wenn er nicht benötigt wird.

Umfassende rechtliche und technische Informationen zum sicheren Einsatz von Funknetzen wird eine in Kürze erscheinende Orientierungshilfe des Arbeitskreises Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder bereitstellen.

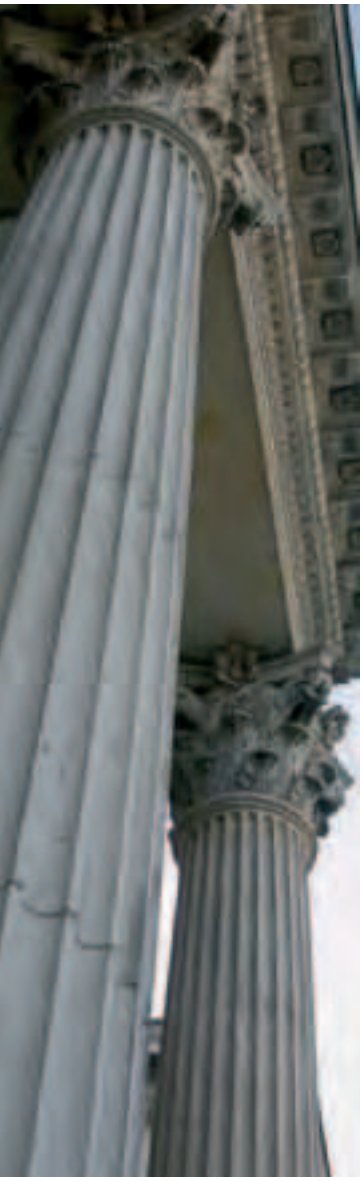
Vertiefende Informationen zum Thema:

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

www.bsi.bund.de (Informationen zu Bluetooth und WLAN)

eGovernment:

Zentrale Herausforderung beim Übergang in die Informations- und Wissensgesellschaft



Es besteht kein Zweifel mehr, dass wir im Informationszeitalter angekommen sind und unsere Gesellschaft sich immer stärker zu einer Wissensgesellschaft entwickelt. Daraus ergibt sich auch eine neue Qualität der Beziehung zwischen Bürger und Verwaltung: Kundenorientierung, Effizienz, Geschwindigkeit und Transparenz gehören zu den Merkmalen, die von einer modernen Verwaltung selbstverständlich erwartet werden, gerade auch durch Nutzung der neuen Informations- und Kommunikationstechnologien.

Auch öffentliche Stellen des Landes Niedersachsen bieten ihre Serviceleistungen zunehmend auf elektronischem Weg an – und damit unabhängig von Zeit, Ort, Besuchsregelungen und Verkehrssituation, ohne größere Wartezeiten, ohne Suche nach den richtigen Kontakten und ohne dass Detailkenntnisse über Verwaltungsaufbau oder -zuständigkeiten notwendig sind. Umfangreiche Online-Informationen über Verwaltungsdienstleistungen, eMail-Erreichbarkeit der Mitarbeiterinnen und Mitarbeiter, zahlreiche Formulardownloads sowie eine Reihe ausgewählter Internetanwendungen erleichtern den Austausch zwischen Bürgern, Wirtschaft und Verwaltung, vereinfachen Verfahrensabläufe und senken die Kosten für die öffentliche Verwaltung. „Nicht die Bürger sollen laufen, sondern die Daten" lautet dabei eine viel gebrauchte Parole. Aber auch innerhalb der Verwaltung ist eine Reorganisation von Arbeitsabläufen und Kommunikationswegen in Gang gesetzt worden. Dokumentenmanagement, Workflow, Wissensmanagement, elektronische Archivierung und virtuelle Zahlverfahren sind die Ziele. Dabei wird von den Bediensteten der öffentlichen Verwaltung zukünftig eine hohe Flexibilität im Umgang mit den neuen Technologien verlangt. Nach den Vorstellungen des Innenministers sollen innerhalb der nächsten zehn Jahre alle geeigneten Behördendienstleistungen in Niedersachsen online zur Verfügung stehen.

Akzeptanz setzt Datenschutz und Datensicherheit voraus!

Die notwendige Akzeptanz für eGovernment-Anwendungen auf Seiten der Bürgerinnen und Bürger sowie der anderen „Kunden" der Verwaltung wird jedoch nur zu erreichen sein, wenn eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz der personenbezogenen Daten gewährleistet ist. Ich habe es mir daher seit meiner Amtsübernahme im Jahr 1999 zur besonderen Aufgabe gemacht, den Prozess des eGovernment aus Datenschutzsicht intensiv und konstruktiv zu begleiten, und viele Vorschläge für datenschutzfreundliche Anwendungen und technisch-organisatorische Begleitmaßnahmen entwickelt.

17

Elektronische Kommunikation im Verwaltungsverfahren

Mit der Novellierung des Verwaltungsverfahrensgesetzes des Bundes vom August 2002 wurde der juristische Boden für das eGovernment in der Form des elektronischen Verwaltungsverfahrens durch den Bund bereitet. Niedersachsen folgt ihm mit einer Änderung seines Verwaltungsverfahrensrechts auf diesem Weg – wenn auch mit ein wenig Verspätung. Die Voraussetzungen für die Nutzung elektronischer Kommunikationswege im Verhältnis Bürger/Verwaltung und für den Erlass elektronischer Verwaltungsakte sind damit geschaffen. Es ist zu erwarten, dass – unabhängig vom Umfang der tatsächlichen Nutzung – kurzfristig die Erwartung an die öffentlichen Stellen herangetragen wird, auch für bisher in Schriftform einzureichende Dokumente einen Zugang für die elektronische Kommunikation zu eröffnen. Die Eröffnung dieses Zugangs setzt erhebliche technische und organisatorische Maßnahmen voraus, damit ein angemessener Datenschutz und die erforderliche Datensicherheit gewährleistet sind. Würde man die technische Ausstattung, die etwa für das Ver- und Entschlüsseln ein- und ausgehender Informationen, für die Signaturprüfung bei rechtserheblichen Dokumenten oder für die Prüfung auf schädliche Inhalte erforderlich ist, die erforderlichen Programme und das zu ihrer Handhabung notwendige rechtliche und technische Know-how dezentral auf allen Arbeitsplätzen in den Verwaltungen vorhalten müssen, ergäbe sich ein völlig unvertretbarer und wohl auch kaum leistbarer finanzieller und kapazitativer Aufwand für Beschaffungen, Pflege und Wissensvermittlung. Daher ist es zwingend geboten, Möglichkeiten für eine Zentralisierung dieser Sicherheitsfunktionen zu entwickeln, die organisatorisch am ehesten mit Funktionen der bisherigen analogen Posteingangsstellen vergleichbar sind.

Virtuelle Poststelle – eine datenschutzgerechte Basiskomponente

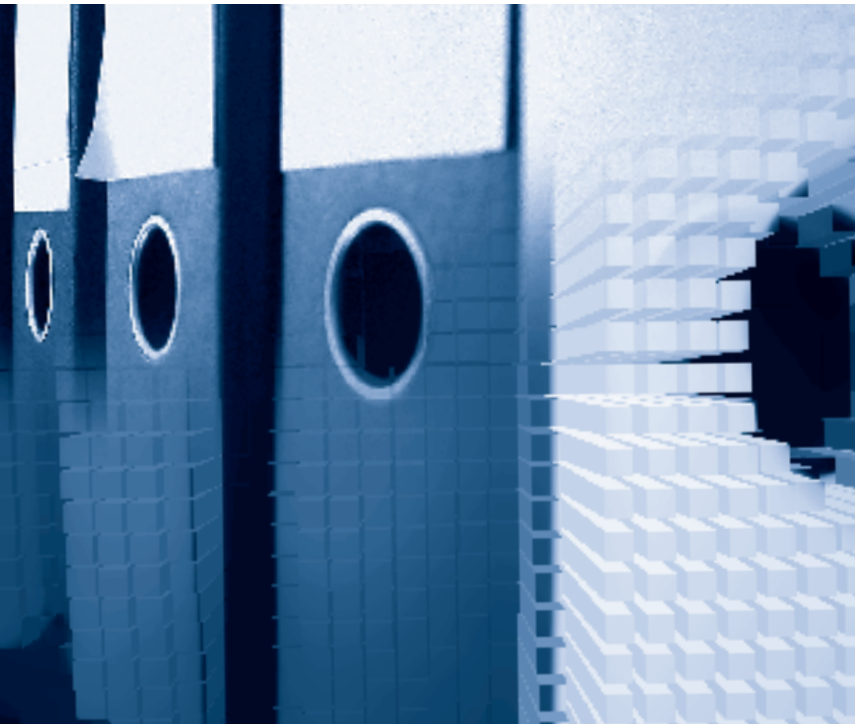
Als Lösung bietet sich die Virtuelle Poststelle (VPS) als Basiskomponente zur Kommunikationssicherheit mit Querschnittsfunktionalität an. Sie stellt über standardisierte Schnittstellen Sicherheitsdienste bereit für die gesicherte Kommunikation zwischen Behörden und externen Kommunikationspartnern wie Bürgern, Wirtschaft und anderen Behörden und fungiert als zentrales Security-Gateway, welches die Funktionen Authentifizierung, Signaturprüfung und Signaturerstellung sowie Ent- und Verschlüsselung zur Verfügung stellt. Die Adressierung erfolgt über Zertifikatsdaten oder andere Metainformationen über die Dokumente, die eine Weiterleitung an die zuständige Stelle (z. B. Sozialamt, Meldeamt) ermöglichen. Als Kommunikationskanäle unterstützt die VPS sowohl eMail- als auch Web-Anwendungen. Weiterhin bedient sie Schnittstellen zu Workflow-, Dokumentenmanagement- und Archiv-Systemen sowie auch zu Fachverfahren. Die Zentralisierung dieser Funktionen erhöht jedoch das Gefährdungspotenzial für das Recht auf informationelle Selbstbestimmung. Unter meiner Federführung ist daher in enger Kooperation insbesondere mit den Kommunalen Spitzenverbänden eine Handreichung erarbeitet worden, die die datenschutzrechtlichen und -technischen Anforderungen, die zu beachtenden Sicherheitsaspekte und die Architektur der VPS als Basiskomponente des eGovernment in praxisnaher Form zusammenstellt. Sie ergänzt die im Dezember 2002 vorgelegten „Handlungsempfehlungen für ein datenschutzgerechtes eGovernment".
Mit der konsequenten Umsetzungen meiner Handlungsempfehlungen könnte die niedersächsische Verwaltung zum Vorreiter für ein bürger- und datenschutzfreundliches eGovernment werden.

Von der Erstellung bis zur Archivierung eines digitalen Dokuments

Die aus dem Projekt „ArchiSig – Beweiskräftige und sichere Langzeitarchivierung digital signierter Dokumente" unter Beteiligung des Nds. Hauptstaatsarchivs und des Informatikzentrums Niedersachsen entwickelten praktischen Umsetzungskonzepte zeigen deutlich auf, dass zukünftig gesetzeskonform, praktikabel und wirtschaftlich digital „archiviert" werden kann. Unterstützt durch dieses Projekt und Entwicklungen beim eGovernment sowie bei der Digitalisierung der Verwaltung soll nun der nächste Schritt folgen:

Dokumenten-Management-Systeme (DMS)

sollen Einzug in die niedersächsischen Verwaltungen erhalten. Projekte wie die „eAkte" im Wirtschaftsministerium sind die ersten Boten der neuen Technologien. Nach den Vorstellungen der handelnden Akteure sollen Informationen jeder Art für „Alle" erschließbar sein. Durch vielfältige Datenverknüpfungen und -kombinationen sowie durch die Erstellung von Hypothesen und deren Überprüfung sollen sogar bisher völlig unbekannte Informationen gewonnen werden.



Schon bei meinen Informationsbesuchen bei großen Softwareanbietern auf der CeBIT 2004 habe ich allerdings festgestellt, dass für die gezielte Zusammenführung von personenbezogenen Daten aus unterschiedlichen Datenquellen und ihre Auswertung programmseitig überwiegend keine Information der Betroffenen vorgesehen ist. Diese Entwicklung schafft neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit. Die Erstellung von Persönlichkeitsprofilen, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung der Daten sind befürchtete Risiken. Da in einem DMS auch personenbezogene Daten der jeweiligen Bearbeiter verarbeitet werden, sehe ich hier auch besondere Gefährdungen und Risiken für die Bediensteten, insbesondere wenn Ergebnisse aus dem Workflow-Management zu einer individuellen Verhaltens- und Leistungskontrolle genutzt werden könnten.

Mir ist jedoch auch deutlich geworden, dass der Einsatz von DMS ein wesentlicher und unverzichtbarer Baustein in der Reihe der Basiskomponenten des eGovernment ist. Ich beabsichtige daher, die weitere Ausformung und Konkretisierung sowie die erforderliche Präzisierung der Zugriffs- und Auswertungsmöglichkeiten der niedersächsischen Projekte aktiv und konstruktiv zu begleiten. Um die erzielten Ergebnisse möglichst transparent aufzuzeigen, werde ich über den Fortschritt im Rahmen eines „Vorab-Controllings“ in meinem Internetangebot aktuell berichten.

Nach den guten Erfahrungen mit „internen“ Projekten (LAN-Firewall, LoHN, Terminal-Servertechnologien, Telearbeit, mobiles Arbeiten) wäre es sehr wünschenswert, für die praktische Erprobung datenschutzgerechter Lösungen ein Pilotfeld für ein DMS zu finden. Förderlich dabei wären Kooperationen mit Partnern aus Verwaltung und Wirtschaft.

Vertiefende Informationen zum Thema:

www.lfd.niedersachsen.de (Themen > eGovernment)

www.bsi.de (Thema: eGovernment-Handbuch – Bundesamt für Sicherheit und Informationssicherheit)

www.bundonline2005.de (Bund Online 2005)

www.koopa.de (Kooperationsausschuss ADV)

www.datenschutz.de (Virtuelles Datenschutzbüro)

www.archisig.de (Informationen zur langfristigen Aufbewahrung vom elektronisch signierten Dokumenten)

www.osci.de (Informationen zum Datenformats- und Datentransport-Standard OSCI, zur OSCI-Leitstelle sowie dem Stand der damit verbundenen Projekte.)

Informationszugang als Konsequenz des Rechts auf informationelle Selbstbestimmung 18

Ist Niedersachsen bald eine Insel?

„Warum wollen Sie das wissen?
Diese Information unterliegt der „Amtsverschwiegenheit"!

In Niedersachsen werden amtliche Informationen noch immer grundsätzlich als „geheim" eingestuft, unabhängig davon, ob sie tatsächlich vertraulich oder schutzbedürftig sind. Die Bürgerinnen und Bürger in Niedersachsen müssen sich immer noch rechtfertigen und ein rechtliches Interesse begründen, wenn sie Auskünfte und Informationen von ihren Behörden verlangen oder Einsicht in amtliche Dokumente nehmen wollen. Diese obrigkeitsstaatliche Praxis wird den Anforderungen einer modernen und demokratischen Informationsgesellschaft nicht gerecht.

Die Erfahrungen in den Bundesländern, in denen schon seit längerem Informationsfreiheits- oder -zugangsgesetze bestehen, sind durchweg positiv. Insbesondere haben sich die Befürchtungen, die Verwaltungen würden unter einer Flut von Anträgen ersticken und kostenmäßig erheblich belastet werden, in keiner Weise bestätigt.

Der Anspruch auf Informationszugang ist mittlerweile Standard in fast allen Mitgliedstaaten der Europäischen Union und auch in den meisten Ländern der Welt. Zuletzt hat auch die Türkei im April 2004 ein Informationszugangsgesetz verabschiedet. Auf Bundesebene soll nun nach langen Vorarbeiten noch vor Jahresende 2004 der längst überfällige Entwurf eines für die Behörden der Bundesverwaltung geltenden Informationsfreiheitsgesetzes in das parlamentarische Verfahren eingebracht werden.

Niedersachsen muss handeln!

Bereits seit längerem appelliere ich an die politisch Verantwortlichen, auch in Niedersachsen ein Informationszugangsgesetz zu erlassen, das den niedersächsischen Bürgerinnen und Bürgern einen verfahrensunabhängigen Anspruch auf Zugang zu amtlichen Informationen und Dokumenten einräumt. Leider ist der Landtag auch unter wechselnden Mehrheiten diesem Appell bisher nicht gefolgt. Nachdem nun für die Bundesverwaltung ein Informationszugangsgesetz auf den Weg gebracht werden wird, muss auch in Niedersachsen gehandelt werden. Unterschiede im Zugriff auf behördliche Informationen je nachdem, ob es sich um eine Bundes- oder um eine Landes- und Kommunalbehörde handelt, sind unvertretbar und den Bürgerinnen und Bürgern nicht zu vermitteln.

Vertiefende Informationen zum Thema:

www.informationsfreiheit.de
www.datenschutzzentrum.de/informationsfreiheit
www.pro-information.de

Dienstleister für Verwaltung und Wirtschaft:

Meine Angebote und Produkte

Mit dem Inkrafttreten der Novelle zum Niedersächsischen Datenschutzgesetz habe ich seit Juni 2001 die Pflicht, die Öffentlichkeit über bedeutsame Entwicklungen auf dem Gebiet des Datenschutzes auch unabhängig von der Vorlage des Tätigkeitsberichtes zu informieren. In der Praxis erfülle ich diese Informationspflicht vor allem durch die Herausgabe von Orientierungshilfen und Handlungsanleitungen, durch ein breites Informations- und Beratungsangebot im Internet, durch die Einrichtung von Diskussionsforen und elektronisch unterstützten Netzwerken mit den behördlichen und betrieblichen Datenschutzbeauftragten sowie durch eine umfangreiche Beratungs-, Vortrags- und Fortbildungstätigkeit aller Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle. Mit dem 2003 neu errichteten Datenschutzinstitut Niedersachsen habe ich die Fortbildungsaktivitäten in einer eigenen Einrichtung gebündelt und erheblich ausgeweitet. Flyer mit prägnanten Kurzinformationen vervollständigen mein Informations-Angebot. Sie erläutern die Datenschutzthemen mit kurzen verständlichen Statements. Eine umfangreiche rechtliche Würdigung oder die detaillierte Beschreibung einer technischen Lösung ist nicht beabsichtigt, vielmehr soll Datenschutzbewusstsein geweckt werden.

Broschüren, Orientierungshilfen, Checklisten, FAQ's, Flyer …

Mit meinen Informationsbroschüren, Handreichungen, Orientierungshilfen und Checklisten will ich alle diejenigen erreichen, die in Verwaltung und Wirtschaft an zentraler Stelle als Führungskräfte, als Organisatoren, als Verfahrensentwickler, als IT-Verantwortliche, als interne Datenschutzbeauftragte oder als Personalvertretungen/Betriebsräte datenschutzgerechte Anwendungen vorbereiten oder schon umsetzen. Ich wende mich aber natürlich auch an Mitarbeiterinnen und Mitarbeiter in Verwaltung und Wirtschaft. Für Nutzerinnen und Nutzer sind die Hinweise und Empfehlungen besonders wichtig, die sich auf Instrumente zum Selbstdatenschutz beziehen. Denn ein Teil der Verantwortung für den Schutz und die Vertraulichkeit ihrer Daten verbleibt auch weiterhin bei den Betroffenen selbst und kann auch nur von ihnen durch Nutzung der beschriebenen Selbstschutzinstrumente ausgefüllt werden.

Drei Beispiele sollen verdeutlichen, dass diese schriftlichen oder im Internet abrufbaren Informationsangebote auch die tägliche Arbeit in der Geschäftsstelle sehr erleichtern:

- Eine Behörde plant den Anschluss seines LAN ans Intranet/Internet und erfragt Sicherungs-Maßnahmen, um vertrauliche Kommunikation durchführen

zu können. Ein großer Teil der Fragen kann mit der Zusendung der betreffenden Orientierungshilfen und Checklisten schnell und kostengünstig beantwortet werden.

- Ein behördlicher Datenschutzbeauftragter erfragt die rechtlichen, technischen und organisatorischen Grundlagen seiner Aufgaben, um sich zu qualifizieren und die für eine Übernahme der Funktion im Gesetz festgelegten Voraussetzungen zu erfüllen. Während früher umfangreicher Schriftverkehr zur Beantwortung der Fragen erforderlich war, dient den Datenschutzbeauftragten nun das Informationsblatt „Aufgaben und Stellung des behördlichen Datenschutzbeauftragten“ als Hilfsmittel.
- Eine Behörde beabsichtigt den Weg ins eGovernment vorzube möchte sich im Vorfeld über gesetzliche Regelungen, Datensicherungsmaßnahmen und über datenschutzgerechte Referenzanwendungen informieren. Auch hier bietet die vorhandene Broschüre „Datenschutzgerechtes eGovernment“ wertvolle Hilfe.

Meine Veröffentlichungen werden in kleiner Auflage gedruckt. Sie werden nach individuellen Verteilern versandt und können von Interessierten bei mir auch direkt angefordert werden. Alle Veröffentlichungen werden komplett auch in mein Internetangebot eingestellt; sie sind so im Download jederzeit und schnell erhältlich.

Neuerscheinungen der letzten Zeit: Den Selbstdatenschutz in den Mittelpunkt gestellt!

- Datenschutz in der Arztpraxis – Förderung von Vertraulichkeit und Datenschutz (vgl. dazu unter Nr. 9)
- Neuauflage der Kommentierung zum NDSG
- Datenschutzgerechtes Internetangebot der Wirtschaft
- „Achtung Kamera!“ – Videoüberwachung im nichtöffentlichen Bereich (vgl. dazu unter Nr. 10)
- Rechte der Kunden – Immer eine Antwort auf Fragen (FAQ) (vgl. dazu unter Nr. 12)

www.lfd.niedersachsen.de: Niedersachsens Nr. 1 auf dem Gebiet des Datenschutzes

Seit Anfang 1998 ist der LfD im Internet mit einem selbstgestalteten Informationsangebot vertreten. Das Internet-Angebot umfasst Pressemitteilungen, die Tätigkeitsberichte, datenschutzrelevante Rechtsvorschriften und Urteile, Beschlüsse der DSB-Konferenzen, Info-Blätter, Empfehlungen, Orientierungshilfen, Checklisten und sonstige Info-Materialien. Darüber hinaus stehen ich und meine Mitarbeiterinnen und Mitarbeiter über die angebotene eMail-Kommunikation für Datenschutzfragen jederzeit mit Tat und Rat zur Verfügung. Dieser Service wird in erfreulich hoher Zahl von Wirtschaft und Verwaltung sowie von Bürgerinnen und Bürger genutzt. Täglich werden ca. 1.000 Seiten des Internet-

Angebots gelesen und ca. 10 Orientierungshilfen und Checklisten zur Selbstkontrolle heruntergeladen. Das bisherige Feedback zeigt, dass das Internet-Angebot überwiegend von Fachleuten oder Institutionen mit den Aufgabenfeldern Datenschutz und Datensicherheit genutzt wird. Um auch interessierte Bürger und Bürgerinnen sowie Journalisten auf die Homepage des LfD zu „locken", beabsichtige ich, zukünftig verstärkt verständliche Kurzinformationen und Aussagen zu tagesaktuellen Themen anzubieten.

Selbstdatenschutz: Der PC-Selbsttest für jedermann!

Mit dem PC-Selbsttest können Sie online Ihren privaten Personal Computer auf sichere Browser-Einstellungen und mögliche Sicherheitslücken hin überprüfen. Sie erhalten Hinweise auf angemessene Sicherheitseinstellungen sowie Tipps für weitergehende Informationen über mögliche Gefahren und deren Vermeidung. Der Selbsttest wird in meinem Auftrag auf einem geschützten Server der Fachhochschule Nordostniedersachsen in Lüneburg durchgeführt. Eingaben und Ergebnisse werden verschlüsselt übertragen. Der PC-Selbsttest wird in drei Phasen durchgeführt, die einzeln angewählt werden. In Phase 1 werden alle verfügbaren Browser-Informationen ermittelt (Verbindung Proxy-Server, Adresse des Proxy-Servers, Adresse Ihres Rechners, Name Ihres Rechners, Browser, Betriebssystem). Weiter wird getestet, welche Funkionen aktiviert sind (Cookies, JavaScript, Java, sicheres ActiveX, unsicheres ActiveX, VFScript). In Phase 2 wird versucht, eine Netzverbindung zum Rechner aufzubauen und Windows- bzw. Samba-Freigaben zu ermitteln. In Phase 3 werden offene Ports gescannt.
Ich beabsichtige, den Selbsttest zukünftig in einer Kooperation mit dem Heise-Verlag zusammen mit weiteren Testmöglichkeiten inhaltlich zu aktualisieren und neu zu gestalten.

Ein virtuelles Netzwerk: Das „Forum für Datenschutz"

„Darf der Bürgermeister einer Gemeinde dem Verwaltungsausschuss eine namentliche Liste aller Grundstückseigentümer vorlegen, damit überprüft werden kann, ob für diese Eigentümer die richtige Grundsteuer erhoben wird? Steht einer solchen Auskunft das Steuergeheimnis entgegen?"

„Unsere Dienstelle will die Dienstanweisung für den Datenschutz überarbeiten! Wer kann mir eine aktuelle Muster-Dienstanweisung zur Verfügung stellen?"

Solche und ähnliche Fragen und Anforderungen stellen sich den behördlichen Datenschutzbeauftragten täglich neu. Um hier rasch und unkompliziert Hilfestellungen anzubieten, habe ich auf meiner Homepage das „Forum für Datenschutz" eingerichtet. Es bietet allen behördlichen Datenschutzbeauftragten der Landes- und Kommunalverwaltung sowie allen Beschäftigten der öffentlichen Verwaltung, die sich für den Datenschutz in ihren Dienststellen interessieren, die Möglichkeit, Meinungen und Informationen zu allen Fragen des Datenschutzes und der Datensicherheit auszutauschen sowie gemeinsam datenschutzgerechte Lösungen zu suchen. Neben einem „Öffentlichen Forum", das allen Interessierten zur Verfügung steht, wurden darüber hinaus Fachforen, so etwa für die behördlichen Datenschutzbeauftragten der Landes- und Kommunalveraltung, den Justizvollzugsbereich und die Polizei eingerichtet. In diesen Fachforen können in geschlossenen Benutzergruppen „geschützt" fachspezifische Fragestellungen erörtert werden. Die Foren können gerade für die behördlichen Datenschutzbeauftragten, die ihre Funktion vor Ort in den Dienststellen oftmals im Nebenamt als „Einzelkämpfer" wahrnehmen, eine wertvolle Hilfe sein.

Datenschutzinstitut Niedersachsen (DiN): Kompetent qualifiziert!

Ein neues Angebot zur Vermittlung von Datenschutzwissen und Erkenntnissen aus der praktischen Arbeit ist das Datenschutzinstitut Niedersachsen (DiN). Es versteht sich als ein Forum, das bedarfs- und kundenorientierte Fortbildung für Verwaltung und Wirtschaft sowie für Bürgerinnen und Bürger des Landes Niedersachsen in Fragen des Datenschutzes und der Datensicherheit anbietet. Die Schulungen vermitteln zeitnah und umfassend Wissen über Forderungen, Empfehlungen, beispielhafte Lösungen und Werkzeuge zum Thema Datenschutz und Datensicherheit. Angeboten werden spezielle Kurse und Workshops zu allgemeinen oder bereichsspezifischen datenschutzrechtlichen Fragen und zur technischen Datensicherheit. Das Schulungsprogramm reagiert flexibel auf aktuelle Entwicklungen und den Bedarf der Klientel aus Wirtschaft und Verwaltung. Darüber hinaus werden Informations- und Unterstützungswünsche von Bürgerinnen und Bürgern erfüllt. Das Schulungsangebot ist als spezielle Erweiterung zu den Angeboten anderer Fortbildungsträger zu verstehen. Als Referenten kommen Mitarbeiterinnen und Mitarbeiter der Geschäftsstelle zum Einsatz, die diese Aufgaben als Teil ihres Hauptamtes erfüllen, so dass keine Referentenhonorare anfallen. Neben dem eigentlichen Schulungsbetrieb wird das DiN

auch für Veranstaltungen genutzt, mit denen einzelfallübergreifend Verständnis und Akzeptanz von Datenschutz gefördert werden soll (z. B. für Gesprächskreise mit Führungskräften aus Wirtschaft und Verwaltung, um Rückkopplungsebenen und Rollenverständnis zu schaffen). Alle Veranstaltungen des DiN werden in einem Programmheft veröffentlicht. Neu ist die Möglichkeit, das erforderliche Basiswissen behördlicher und betrieblicher Datenschutzbeauftragter in einer Kursreihe zu erwerben und mit einem DiN-Zertifikat abzuschließen. Das DiN hat sich gut etabliert, schon im zweiten Jahr seines Bestehens sind viele Kurse aus- und überbucht.

CeBIT: Der besondere Datenschutztag – Herzlich willkommen!

Es ist Tradition geworden, dass ich auf der CeBIT in Hannover – dem weltweit größten Schauplatz der Informations- und Kommunikationstechnologie – ein Forum zum Datenschutz veranstalte, das seit letztem Jahr in einen Datenschutz-Tag eingebettet ist. Im Jahr 2004 haben mehr als 100 Teilnehmer aus Verwaltung und Wirtschaft das Forum besucht, das unter den Titel „Schöne digitale Welt – bleiben Privatsphäre und Individualität auf der Strecke?“ gestellt war. In Form von Vorträgen und Streitgesprächen wurden der Datenschutz in der Telekommunikation und der Einsatz von Funk-Chips und Smart-Labels auf der Grundlage der RFID-Technik erörtert und gemeinsam mit Experten diskutiert. Darüber hinaus ist auf Marktständen über aktuelle Problemstellungen des Datenschutzes und über datenschutzgerechte Lösungsansätze informiert worden. Aktuelle Informationen über den Datenschutztag auf der CeBIT 2005 am 14. März 2005 finden Sie in meinem Internetangebot.

Kooperationen, Netzwerke, Bündnisse … Zusammenarbeit mit Dritten!

Das Thema Datenschutz erweckt in der Öffentlichkeit immer dann Interesse, wenn es um aktuelle Themen und Fragen geht und wenn der Datenschutz Bündnisgenossen hat. Der Arbeitskreis der Datenschutzbeauftragten der Hochschulen, der Erfa-Kreis der betrieblichen Datenschutzbeauftragten, die Kommunalen Spitzenverbände, die Kommunalen Studieninstitute Hannover, Braunschweig und Oldenburg, die Universität Hannover, die Kommunalen Datenzentralen, das Bundesamt für Sicherheit in der Informationstechnik (BSI), das Informatikzentrum Niedersachsen (IZN), die Datenschutz Nord GmbH, die Ärzte- und Zahnärztekammer, die Psychotherapeutenkammer, die Kassenärztliche Verreinigung, der Einzelhandelsverband, die Gesellschaft für Datenschutz und Datensicherheit, die Industrie- und Handelskammern, die NordLB, VW, BHW und der Niedersächsische Sparkassen- und Giroverband sind solche Bündnispartner, mit denen ich in den Jahren 2003/2004 mit großem Erfolg Projekte und Veranstaltungen durchgeführt habe.

Die Suche nach und die Kooperation mit Bündnispartnern aus Wirtschaft, Verwaltung und Verbänden werden auch zukünftig ein wichtiger Teil meiner Tätigkeit sein, weil auf diese Weise Kräfte gebündelt und Synergien geschöpft werden können.

Rückschau

Im XVI. Tätigkeitsbericht für die Jahre 2001/2002 habe ich im Kapitel 2 für 13 Bereiche den aus meiner Sicht für den Gesetzgeber, die Landesregierung bzw. das zuständige Ressort bestehenden datenschutzrechtlichen Handlungsbedarf benannt. In der folgenden Rückschau wird dargestellt, ob und in welcher Weise meine Erwartungen und Forderungen zwischenzeitlich aufgenommen worden sind:

1. Forderung:

Parallel zu den Erörterungen im Bund sollte in Niedersachsen die Diskussion zur grundlegenden Modernisierung des Datenschutzrechts frühzeitig aufgenommen und so geführt werden, dass Niedersachsen im Bund-Länder-Abstimmungsverfahren und bei den Beratungen des Bundesrates eine aktive Mitgestaltungsrolle übernehmen kann.

Sachstand: Die Erörterungen zur grundlegenden Modernisierung des Datenschutzrechts sind im Bundesbereich seit November 2003 nicht mehr weitergeführt worden, daher ist die Forderung nach einer parallelen Diskussion in Niedersachsen derzeit nicht aktuell.

2. Forderung:

Nach dem Vorbild Schleswig-Holsteins sollten – zur Förderung von eGovernment in der niedersächsischen Verwaltung – baldmöglichst im NDSG Regelungen zur datenschutzrechtlichen Auditierung von Behörden oder Behördenteilen sowie zu einem Gütesiegel für IT-Produkte, die in der öffentlichen Verwaltung zum Einsatz kommen, verankert werden.

Sachstand: Die Forderung, die auch Gegenstand eines Entschließungsantrages der Fraktion Bündnis 90/DIE GRÜNEN vom 16.04.2002 (LT-Drs. 14/3326) war, ist im politischen Raum abgelehnt worden.

3. Forderung:

Die Arbeiten zur Schaffung eines Informationszugangsgesetzes sollten in Niedersachsen möglichst zeitlich parallel zum Gesetzgebungsverfahren im Bund kurzfristig wieder aufgenommen werden.

Sachstand: Die Forderung ist wieder aktuell geworden, nachdem für die Bundesverwaltung der Entwurf eines Informationszugangsgesetzes nunmehr kurzfristig auf den Weg gebracht werden soll (vgl. dazu auch unter Nr. 18).

4. Forderung:

Um für die Verwaltungspraxis keine weiteren Verunsicherungen zu erzeugen, sollte in der Frage der Notwendigkeit einer gesetzlichen Grundlage für Videoüberwachungsmaßnahmen öffentlicher Stellen rasch ein Konsens zwischen Landesregierung und LfD gesucht werden, in dessen Rahmen auch geklärt werden muss, welche Bedeutung in diesem Zusammenhang dem so genannten Hausrecht zukommt.

Sachstand: Die Forderung ist durch den Gesetzesvorschlag zur Einfügung einer mit mir abgestimmten Regelung zur Videoüberwachung in § 25a NDSG erfüllt.

5. Forderung:

Im Rahmen der zentralen IT-Koordinierung des Landes sollten die Überlegungen forciert werden, zur Verbesserung der Datensicherheit modernere Chipkarten-Systeme einzusetzen, die auch eine hierarchische Struktur von Gruppenschlüsseln unterstützen.

Sachstand: Der Vorschlag wurde von der Arbeitsgruppe „Elektronische Signatur" des Landes aufgenommen. Er soll technisch umgesetzt werden, sobald dies herstellerseitig durch entsprechende neue Chipkartenmodelle unterstützt wird. Zudem plant die niedersächsische Landesverwaltung, für diese Einsatzfelder eine eigene Zertifikatsstruktur aufzubauen. Die Arbeiten werden weiter von mir begleitet.

6. Forderung:

Bei der inhaltlichen Ausgestaltung der so genannten Neuen Medienordnung sollten die bewährten dezentralen Strukturen bei der Aufsicht über die Diensteanbieter nur behutsam durch Instrumente der Selbstregulierung und einer zentralen Koordinierung ergänzt werden.

Sachstand: Die Arbeiten des Bundes an einem „Elektronische Medien-Datenschutzgesetz", in dessen erstem Entwurf insoweit problematische Regelungen enthalten waren, sind nicht fortgeführt worden.

7. Forderung:

Die Bedingungen für die datenschutzgerechte Nutzung von Internet und eMail an den Arbeitsplätzen in der öffentlichen Verwaltung sollten auf der Grundlage der von den Datenschutzbeauftragten entwickelten Orientierungshilfe in einer Vereinbarung mit den Spitzenorganisationen der Gewerkschaften nach § 81 Nds. PersVG festgeschrieben werden.

Sachstand: Die Landesregierung hat in ihrer Stellungnahme zum XVI. Tätigkeitsbericht seinerzeit den Abschluss einer Vereinbarung nach § 81 Nds. PersVG abgelehnt und an dieser Haltung bis heute festgehalten.

8. Forderung:

Die Umsetzung der rahmenrechtlichen Vorgaben des novellierten Melderechtsrahmengesetzes in das niedersächsische Landesrecht sollte baldmöglichst erfolgen; dabei sollten zur Sicherstellung von Datenschutz und Datensicherheit bei Nutzung des elektronischen Weges zusätzliche Vorkehrungen geschaffen werden.

Sachstand: Die Anpassung des niedersächsischen Melderechts steht immer noch aus, obwohl die im Melderechtsrahmengesetz festgelegte Umsetzungsfrist längst abgelaufen ist. Dies behindert auch den Einsatz der in Abstimmung mit mir von den Kommunalen Spitzenverbänden entwickelten datenschutzgerechten Programme für ein elektronisches Meldeverfahren.

9. Forderung:

Die Landesregierung sollte über den Bundesrat initiativ werden, um eine immissionsschutzrechtliche Rechtsgrundlage zum Anlegen eines Katasters über die Standorte von Mobilfunkanlagen und zu Regelungen über die Veröffentlichung von Standortdaten zu schaffen.

Sachstand: Das Umweltministerium geht davon aus, dass Mobilfunksendeanlagen in der Regel für jeden sichtbar seien, so dass durch die Benennung des genauen Standortes nur offenkundige personenbezogene bzw. personenbeziehbare Daten veröffentlicht werden. Die Betroffenen würden somit nicht in ihren Rechten beeinträchtigt. In den wenigen Fällen der nicht sichtbaren Anlagen müsse anhand der konkreten Sachlage im Einzelfall geprüft werden, ob Hinderungsgründe im Sinne von §§ 7 und 8 des Umweltinformationsgesetzes vorliegen (LT-Drs. 14/3585 und 14/3667).

10. Forderung:

Das Justizministerium sollte für Überweisungen von Geldauflagen an gemeinnützige Einrichtungen eine auch anderenorts praktizierte Verfahrensweise übernehmen, bei der den Empfängern der Geldauflage keine unnötigen personenbezogenen Daten übermittelt werden.

Sachstand: Das Justizministerium sieht den durch das Strafverfahrensänderungsgesetz 1999 neu gefassten § 487 Abs. 1 Satz 1 i. V. m. § 483 Abs. 1 StPO als ausreichende Ermächtigungsgrundlage für die Datenübermittlung an. Die Übermittlung der personenbezogenen Daten sei unverzichtbar, da sich anderenfalls die ordnungsgemäße Erfüllung der Auflagen nicht überwachen lasse.

11. Forderung:

Das Verfahren zur Übermittlung von personenbezogenen Informationen volljähriger Schüler von der Schule an die Eltern sollte überdacht und ggf. gesetzlich abgesichert werden.

Sachstand: Durch Art. 1 des Gesetzes zur Verbesserung von Bildungsqualität und zur Sicherung von Schulstandorten vom 02.07.2003 (Nds. GVBl. S. 244) wurde § 55 des Niedersächsischen Schulgesetzes dahingehend geändert, dass die (ehemaligen) Erziehungsberechtigten volljähriger Schülerinnen und Schüler, die das 21. Lebensjahr noch nicht vollendet haben, von der Schule über bestimmte Vorgänge zu unterrichten sind, wenn die Schülerinnen und Schüler nicht widersprochen haben. Über einen Widerspruch, der nicht nur einen Einzelfall betrifft, sind die (bisherigen) Erziehungsberechtigten zu unterrichten.

12. Forderung:

Auf der Grundlage der Ergebnisse der gemeinsamen Arbeitsgruppe Ministerium für Frauen, Arbeit und Soziales/LfD sollte gleich zu Beginn der nächsten Legislaturperiode das Gesetzgebungsverfahren zur Schaffung der erforderlichen Regelungen zum Schutz von Gesundheitsdaten eingeleitet werden.

Sachstand: Die Erarbeitung von Regelungen für ein Niedersächsisches Gesundheitsdatenschutzgesetz in der gemeinsamen Arbeitsgruppe konnte noch nicht abgeschlossen werden; die Einbringung eines entsprechenden Gesetzentwurfs war daher noch nicht möglich.

13. Forderung:

Die Landesregierung sollte alle Bemühungen, auf Bundesebene nunmehr rasch Regelungen für ein Arbeitnehmer-Datenschutzgesetz zu entwickeln und in das Gesetzgebungsverfahren einzubringen, nach Kräften unterstützen.

Sachstand: Durch Priorisierung anderer Gesetzesvorhaben sind die Arbeiten an einem Arbeitnehmerdatenschutzgesetz im federführenden Bundesministerium für Wirtschaft und Arbeit immer wieder zurückgestellt worden.

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

65. Konferenz vom 27./28. März 2003 in Dresden

- Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung
- TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden
- Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik
- Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung
- Zur Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen
- Elektronische Signaturen im Finanzbereich
- Transparenz bei der Telefonüberwachung

Entschließungen zwischen der 65. und 66. Konferenz

- Automatisches Softwareupdate
- Bei der Erweiterung der DNA-Analyse Augenmaß bewahren
- Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation
- Neuordnung der Rundfunkfinanzierung

66. Konferenz vom 25./26. September 2003 in Leipzig

- Gesundheitsmodernisierungsgesetz
- Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Entschließungen zwischen der 66. und 67. Konferenz

- Übermittlung von Flugpassagierdaten an die US-Behörden
- Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

67. Konferenz vom 25./26. März 2004 in Saarbrücken

- Forschungsgeheimnis
- Personennummern
- Automatische Kennzeichenerfassung
- RFIDs
- Akustische Wohnraumüberwachung

68. Konferenz vom 28./29. Oktober 2004 in Saarbrücken

- Neuregelung der akustischen Wohnraumüberwachung
- Gravierende Datenschutzmängel bei Hartz IV
- Entschließung zur Verwaltungsmodernisierung

Unser Leitbild

Datenschutz ist Grundrechtsschutz

Standortbestimmung

Das Grundrecht auf informationelle Selbstbestimmung – der Datenschutz – ist Teil der Würde und Persönlichkeit des Menschen und zugleich elementare Funktionsbedingung eines freiheitlich-demokratischen Gemeinwesens. Es sichert das Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen er seine persönlichen Lebensumstände offenbart. Ergänzt wird dieses Grundrecht durch das Recht auf Informationsfreiheit, das die politische Teilhabe des Einzelnen an der Gemeinschaft sichert und damit ebenso wie das Recht auf informationelle Selbstbestimmung Bestandteil einer auf Grundrechtsverwirklichung abzielenden politischen Ordnung ist.

Kernaufgabe Unser Auftrag ist es, die informationelle Selbstbestimmung und ihre Beachtung im Gemeinwesen einzufordern.

Dafür treten wir ein

Anwalt der Bürgerinnen und des Bürgers Wir vertreten als unabhängige Stelle die Interessen der Bürgerinnen und Bürger bei der Verarbeitung ihrer Daten durch Staat und Wirtschaft.

Datenschutz mit Augenmaß Wir betrachten den Datenschutz nicht isoliert, sondern in Abwägung mit den sonstigen Interessen der Bürgerinnen und Bürger und den anerkannten Zielen der Gemeinschaft. Wir räumen dem informationellen Selbstbestimmungsrecht im Zweifel den höheren Rang ein.

Keine Bevormundung Wir informieren intensiv über die Möglichkeiten, sich durch eigenes Zutun gegen einen Missbrauch seiner Daten zu schützen. Wir respektieren aber die Entscheidungssouveränität jedes Einzelnen und drängen keine überzogene staatliche „Fürsorge“ auf.

Aufgeschlossen für neue Technologien Wir treten dafür ein, dass der Einsatz der Technik nach dem geltenden Recht erfolgt und dass rechtliche Bestimmungen auch zeitnah technische Entwicklungen berücksichtigen. Wir sind neuen Entwicklungen gegenüber offen und setzen uns mit dem technischen und gesellschaftlichen Wandel auseinander. Wir unterstützen die Entwicklung datenschutzfreundlicher Technologien; Datensparsamkeit und Datenvermeidung sind der beste Datenschutz.

Kompetenter Ansprechpartner

Überzeugung, Konfliktfähigkeit Wir versuchen zu überzeugen und einvernehmliche Lösungen zu finden, sind im Konfliktfall aber auch bereit, datenschutzgerechtes Handeln gegen Widerstände durchzusetzen.

Gestaltung, Beratung, Kontrolle Wir gestalten den Umgang mit personenbezogenen Daten in der Gesellschaft intensiv mit. Wir beraten Betroffene über Gefährdungen und Rechte sowie Privatwirtschaft und öffentliche Verwaltung über erforderliche Regelungen und Maßnahmen, auch im Hinblick auf Datensparsamkeit und Datenvermeidung. Wir kontrollieren wirkungsvoll die Einhaltung von Datenschutzvorschriften.

Öffentlichkeit, aktivierender Datenschutz Wir informieren Bürgerinnen und Bürger, Verwaltung und Wirtschaft sowie die Medien aktuell über unsere Erfahrungen, Forderungen und Empfehlungen. Wir unterstützen Bürgerinnen und Bürger sowie Institutionen dabei, sich selbst für den Datenschutz zu engagieren.

Moderne Geschäftsstelle Wir verstehen uns als kompetenter Ansprechpartner für Datenschutz und Datensicherheit, dessen Dienstleistung gern in Anspruch genommen werden soll. Unsere Aufgaben erfüllen wir fachkundig, seriös, schnell, freundlich und wirtschaftlich. Vertrauen und partnerschaftliche Zusammenarbeit bestimmen unser Handeln; Kritikfähigkeit gehört dazu. Wir gestalten die Arbeit in der Geschäftsstelle nach modernen Gesichtspunkten.

Der Landesbeauftragte für den
Datenschutz Niedersachsen