Unterrichtung

Der Niedersächsische Ministerpräsident Hannover, den 27.04.2010

Herrn
Präsidenten des Niedersächsischen Landtages

Hannover

Sehr geehrter Herr Präsident,

als Anlage übersende ich die

> **Stellungnahme der Landesregierung zum XIX. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz Niedersachsen für die Jahre 2007 und 2008** (Drs. 16/1808).

Federführend ist das Ministerium für Inneres und Sport.

Mit vorzüglicher Hochachtung

Christian Wulff

Inhaltsverzeichnis

Vorbemerkung

Der Landesbeauftragte für den Datenschutz Niedersachsen (LfD) hat seinen Tätigkeitsbericht für die Jahre 2007 und 2008 untergliedert in einen Teil über den öffentlichen Bereich, einen Teil über den nicht öffentlichen Bereich (Wirtschaftsbereich) und den Teil über den technisch-organisatorischen Datenschutz, der - wie bereits im Tätigkeitsbericht für die Jahre 2005 bis 2006 - das Schwerpunktthema dieses Berichtes bildet. Gemäß § 22 Abs. 3 des Niedersächsischen Datenschutzgesetzes (NDSG) legt der LfD dem Landtag jeweils für zwei Kalenderjahre einen Tätigkeitsbericht über den Datenschutz im öffentlichen Bereich vor.

Die Verpflichtung zur Berichterstattung für den nicht öffentlichen Bereich ergibt sich aus § 38 Abs. 1 Satz 7 Bundesdatenschutzgesetz (BDSG). Eine Stellungnahme der Landesregierung zu diesen Themen erfolgte bisher regelmäßig nicht, da dies gesetzlich nicht vorgesehen ist. Auch dieses Mal wird nur zu einzelnen ausgewählten Themen des nicht öffentlichen Bereichs Stellung genommen.

Der Bericht des LfD enthält kaum konkrete Beanstandungen, die sich bei seinen Kontrolltätigkeiten im öffentlichen Bereich ergeben haben. Er gibt vielmehr einen Überblick über aktuelle datenschutzrechtlich relevante Themen, stellt hierzu die jeweilige Sach- und Rechtslage dar und zeigt Handlungserfordernisse auf. Der LfD bemängelt lediglich den Umgang mit Daten auf mobilen Datenträgern in einem Einzelfall, fordert eine künftige rechtzeitige Beteiligung beim Aufbau automatisierter IT-Verfahren und mahnt Leitlinien und Richtlinien zur IT-Sicherheit an.

Die Landesregierung nimmt zu den einzelnen Themen in der Reihenfolge Stellung, in der sie im Tätigkeitsbericht dargestellt werden.

In den Vorbemerkungen wird die verstärkte Wahrnehmung des Datenschutzes in der Öffentlichkeit betont, die durch die diversen Datenschutzskandale der vergangenen Jahre hervorgerufen wurde. Hier mahnt der LfD z. B. konkrete Regelungen zum Arbeitnehmerdatenschutz an. Die Datenschutzverstöße aus den Jahren 2008 und 2009 insbesondere in verschiedenen Großunternehmen haben deutlich gemacht, dass besonderer Handlungsbedarf beim Datenschutz im Arbeitsleben besteht. Hierzu wurde als ein erster Schritt mit dem Gesetz vom 14.08.2009 eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten verfasst (§ 32 BDSG). Weitere Regelungen sollen folgen. Näheres wird im Abschnitt zum nicht öffentlichen Bereich erläutert.

Die Landesregierung unterstützt die Forderung des LfD, die Bevölkerung verstärkt auf die Risiken im Umgang mit personenbezogenen Daten hinzuweisen. Diese Risiken haben sich durch die zunehmende Nutzung verschiedener Technologien (z. B. Video, Handy, Internet) erheblich erhöht. Hier besteht Aufklärungsbedarf zum verantwortungsvollen Umgang mit den eigenen Daten. Hierzu wird auch auf die Ausführungen in Abschnitt 3 zum aktiven Selbstdatenschutz verwiesen.

Besonders die Innovationen im IT-Bereich verlangen eine kritische Prüfung, ob datenschutzrechtliche Belange jeweils ausreichend berücksichtigt werden. Das technisch Mögliche ist dabei nicht immer mit den Vorgaben der datenschutzrechtlichen Bestimmungen zu vereinbaren. Die Landesregierung wird in ihrem Zuständigkeitsbereich auch in Zukunft darauf achten, dass diese Bestimmungen eingehalten werden und das Recht auf informationelle Selbstbestimmung gewahrt und neben sicherheitspolitischen wie auch wirtschafts- und sozialpolitischen oder gesellschaftlichen Belangen angemessen berücksichtigt wird.

Um diesem Handlungsbedarf gerecht zu werden, hat die Landesregierung mit Beschluss vom 03.03.2009 den Datenschutz im nicht öffentlichen Bereich in Niedersachsen deutlich gestärkt

– durch eine organisatorische Neuordnung der Geschäftsstelle des LfD, durch die der Datenschutz im nicht öffentlichen Bereich zu einer gleichwertigen zweiten Säule neben der des öffentlichen Bereiches ausgebaut wurde,

– durch die Verdopplung des Personals im Datenschutz des nicht öffentlichen Bereichs von fünf auf zehn Stellen mit einer eigenständigen Leitung und

– durch eine konzeptionelle Neuausrichtung der Tätigkeiten des LfD in diesem Bereich.

Im bundesweiten Vergleich liegt Niedersachsen mit dieser Personalausstattung im nicht öffentlichen Bereich im oberen Drittel. Dieser Wert wird allerdings relativiert durch die hohe Bevölkerungs-

zahl als viertgrößtes Bundesland. Dabei ist aber zu berücksichtigen, dass ein flächendeckender Einsatz der Mitarbeiter des LfD in keinem Fall erfolgen kann. Wichtiger sind effiziente Konzepte mit einer zielorientierten und branchenangepassten Beratungsstrategie, die Nutzung von Multiplikatoren, Bildung von Netzwerken und eine wirksame Information und Sensibilisierung der Bevölkerung, insbesondere Jugendlicher.

Es bleibt abzuwarten, ob und welche Veränderungen organisatorischer und rechtlicher Art sich aus dem Urteil des Europäischen Gerichtshofs (EuGH) vom 09.03.2010 ergeben. Der EuGH hat mit dem Urteil festgestellt, dass die Bundesrepublik Deutschland durch die derzeit geltende Regelung zur Datenschutzaufsicht im nicht öffentlichen Bereich gegen die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr verstößt, da die Unabhängigkeit der Kontrollstellen nicht hinreichend gewährleistet ist. Derzeit prüfen die Bundesländer gemeinsam mit dem Bundesministerium für Inneres, welche Konsequenzen aus dem Urteil im Hinblick auf die organisatorische Anbindung der Kontrollstellen zu ziehen sind. Dies gilt auch für Niedersachsen, wo der LfD derzeit gemäß § 22 Abs. 6 NDSG der Fachaufsicht des Ministeriums für Inneres, Sport und Integration unterliegt.

1. Datenschutz im öffentlichen Bereich

Zusammenarbeit mit den kommunalen Datenschutzbeauftragten

Auch die kommunalen Spitzenverbände bestätigen wesentliche positive Effekte für eine landesweit effiziente und gesetzeskonforme Aufgabenwahrnehmung beim Datenschutz durch die Zusammenarbeit der kommunalen behördlichen Datenschutzbeauftragten mit dem LfD. In seinem Bericht hebt der LfD deren Arbeit im Netzwerk Nordwest hervor, die wirksam zur Stärkung und Verbesserung des Datenschutzes in den Kommunen beiträgt. Bei diesem Erfahrungsaustausch sei deutlich geworden, dass eine wirksame Aufgabenwahrnehmung der behördlichen Datenschutzbeauftragten nur bei ausreichender Freistellung von anderen Tätigkeiten möglich sei. Auch aufgrund des Aufgabenzuwachses durch zunehmende E-Government-Verfahren sei es wichtig, die behördlichen Datenschutzbeauftragten in ihrer Arbeit durch ausreichende Freistellungen zu unterstützen. Die Freistellung obliegt den Kommunen im Rahmen ihrer Personal- und Organisationshoheit. Der erforderliche Umfang wird sich dabei nur individuell abhängig von der Situation und den aktuellen Aufgaben vor Ort feststellen lassen.

Gesprächskreis mit Leitern der Rechenzentren und anderen IT-Führungskräften

Auf der Ebene niedersächsischer Hochschulen hat sich die Zusammenarbeit in der „Arbeitsgemeinschaft Datenschutzbeauftragter Niedersächsischer Hochschulen“ bewährt. In diesem Zusammenhang wird die Einrichtung des Gesprächskreises mit Leitern der Rechenzentren und anderen IT-Führungskräften begrüßt, an dem auch Hochschulen und Fachhochschulen teilnehmen.

Das Niedersächsische Beamtengesetz

Mit der Novellierung des Niedersächsischen Beamtengesetzes (NBG) zum 01.04.2009 gelten beim Schutz personenbezogener Daten für Beamte andere Regelungen als für Tarifbeschäftigte (Arbeiter und Angestellte) des öffentlichen Dienstes. Für den letztgenannten Personenkreis hatte der bis zum 31.03.2009 geltende § 261 NBG die Vorschriften über die Verarbeitung von Daten von Beamten (§§ 101 bis 101 h NBG) für anwendbar erklärt.

Für Beamte sind seit dem 01.04.2009 die Regelungen des NBG (§§ 88 ff.) und des Beamtenstatusgesetzes (§ 50) zu beachten. Für Tarifbeschäftigte enthält der Tarifvertrag für den öffentlichen Dienst der Länder (TV-L) Regelungen zum Datenschutz.

§ 3 Abs. 6 TV-L regelt in Satz 1 sowohl das Einsichtsrecht in die Personalakte als auch in Satz 4 und 5 das umfassende Anhörungsrecht der Beschäftigten sowie die Möglichkeit der Beschäftigten zur Stellungnahme für Eintragungen in die Personalakte. Im Übrigen gelten für die Tarifbeschäftigten die von der Rechtsprechung des Bundesarbeitsgerichts (BAG) entwickelten Grundsätze zum Schutz von Arbeitnehmerdaten (z. B. Entscheidung des BAG vom 12.09.2006 - 9 AZR 271/06 - zur Aufbewahrung von sensiblen Gesundheitsdaten in der Personalakte eines Arbeitnehmers oder Urteil des BAG vom 18.11.2008 - 9 AZR 965/07 - zum Anspruch eines Arbeitnehmers auf Entfernung einer dienstlichen Beurteilung aus der Personalakte bei fehlerhaftem Beurteilungsverfahren). Darüber hinaus gelten die Vorschriften des NDSG.

Ein hinreichender Schutz der Rechte der Tarifbeschäftigten ist damit gewährleistet. Eine Regelungslücke beim Schutz personenbezogener Daten der Beschäftigten ist nicht ersichtlich.

Medienkompetenz in der Schule

Angesichts der rasanten Entwicklung audiovisueller Medien und neuer Technologien wird die Vermittlung von Medienkompetenz zur Grundvoraussetzung für eine vollwertige Teilhabe an der gesellschaftlichen Entwicklung. Sie wird zur Schlüsselqualifikation für berufliche Perspektiven und eröffnet neue Bildungshorizonte. Dies gilt besonders für Kinder und Jugendliche, die eine Gruppe der Hauptnutzer der neuen Medien darstellen, aber aufgrund fehlender Erfahrungen oft sorglos ihre persönlichen Daten dort freigeben. Die Landesregierung sieht es daher als ihre Aufgabe an, insbesondere Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren und ihr Datenschutzbewusstsein zu stärken. Die Aktivitäten der Landesregierung wurden ausführlich in der Antwort der Landesregierung auf die Große Anfrage der Fraktion der SPD (Drucksache 16/1480) dargestellt. Wichtig ist bei dieser Aufgabe das Zusammenspiel der verschiedenen Stellen. Hierzu finden regelmäßige Abstimmungs- und Koordinierungsgespräche statt zwischen den zuständigen Ressorts, der Landesmedienanstalt und weiteren Behörden und Stellen. Ein Beispiel für die erfolgreiche Zusammenarbeit (Lehrfilm für Schulen und sonstige Bildungsträger) wurde vom LfD in seinem Tätigkeitsbericht ausdrücklich erwähnt.

Die elektronische Gesundheitskarte

Die Tests mit Versicherten, Arztpraxen, Apotheken und dem Klinikum Wolfsburg zur elektronischen Gesundheitskarte (eGK) sind im Jahr 2008 angelaufen und dienen dazu, die möglichen Anwendungen der Karte im Echtbetrieb aufzuzeigen und auftretende Probleme herauszuarbeiten und, soweit möglich, auszuschalten.

Die Testergebnisse aller inzwischen auf sechs reduzierten Regionen in Deutschland (Heilbronn nimmt seit dem 01.01.2010 nicht mehr teil) wurden zusammengeführt und ausgewertet. Bei der eGK handelt es sich anders als bei der bisherigen Krankenversichertenkarte um eine Mikroprozessorkarte mit Betriebssystem und frei konfigurierbaren Anwendungen und Sicherheitsfunktionen. Die Verwaltung der Versichertenstammdaten gehört zu den nach § 291 a SGB V geforderten Pflichtanwendungen. Die Übernahme der Versichertenstammdaten von der eGK in die Praxisverwaltung erfolgte ohne Probleme.

Allerdings gestaltete sich die Ausstellung der elektronischen Verordnungen im Praxisalltag als sehr zeitaufwändig, sodass einige Apotheken zurzeit nicht mehr an den Testverfahren zur eGK teilnehmen. Zudem führte der Austausch der Konnektoren in einigen Arztpraxen dazu, dass technisch keine eRezepte mehr geschrieben werden können. Das Bundesministerium für Gesundheit hat mittlerweile das Vorhaben, die elektronische Verordnung gleichzeitig mit der Einführung der eGK einzuführen, zunächst verschoben.

Trotz des Beschlusses, die eGK in einer stark abgespeckten Version einzuführen, ist die Speicherung eines Notfalldatensatzes für die Patientinnen oder Patienten, sofern gewünscht, weiterhin vorgesehen und wird sowohl von den Ärztinnen und Ärzten, als auch von den Patientinnen und Patienten grundsätzlich begrüßt. In den Praxistests wurde dies aufgrund des erhöhten Zeitaufwandes bisher jedoch selten angewandt.

Die ständige Verbesserung des Anwenderprozesses findet vor allem aufgrund der Testergebnisse in den sechs Testregionen statt. Dabei hat sich der Prozessablauf in den Arztpraxen z. B. durch die Einführung der Mehrfachsignatur erheblich vereinfacht. Auch der Umgang mit der PIN durch die Patientinnen und Patienten wurde aufgrund der Verlängerung des Zeitfensters von 10 auf 30 Sekunden anwenderfreundlicher. Ein großer Fortschritt wurde dadurch erreicht, dass sich die Kartenherausgeber auf ein einheitliches PIN-Verfahren geeinigt haben.

Im Oktober 2009 hat der sogenannte Basis-Rollout in der Region Nordrhein begonnen, d. h. die eGK wird dort flächendeckend eingeführt. Ziel des Rollouts ist, die Funktionalität der eGK sanft in den Praxisalltag zu migrieren und vor Ort im Praxisalltag auftretende Probleme auszuräumen. Zu diesem Zweck wurde eine Themenlandkarte entwickelt, die eine Übersicht der im Basis-Rollout re-

levanten Themen für alle Projektpartner bietet und helfen soll, Probleme noch zielgerichteter zu lösen.

Nach erfolgreicher Einführung der eGK in der Region Nordrhein wird der Basis-Rollout in zwei Phasen auf ganz Deutschland ausgeweitet. In der ersten Phase werden zunächst die Leistungserbringer mit den Kartenterminals ausgestattet. In der zweiten Phase erfolgt die Ausgabe der neuen eGK.

In Niedersachsen ist beabsichtigt, weiterhin Tests in der Region Wolfsburg durchzuführen. Die eGK soll letztendlich zu einer Verbesserung der Wirtschaftlichkeit, Transparenz und Qualität der Behandlung von Patientinnen und Patienten führen.

Bezogen auf den Datenschutz haben die folgenden Grundsätze weiterhin höchste Priorität:

– Datensparsamkeit und Datentrennung in den Komponentendiensten,

– Anonymisierung und Pseudonymisierung,

– Selbstdatenschutz durch z. B. eigenständige Rechtevergabe und Auskunftsrechte,

– Transparenz und Selbstbestimmung bei jeder Kommunikation sowie Freiwilligkeit der Nutzung,

– Transparenz schaffende Maßnahmen und Funktionen und

– Umgebungen und Verfahren für die aktive Wahrnehmung der Beteiligtenrechte.

Das ELENA-Verfahren

Mit dem ELENA-Verfahrensgesetz vom 28.03.2009 wurde das SGB IV dahingehend erweitert, dass ab dem 01.01.2010 alle Arbeitgeber verpflichtet sind, die Entgeltdaten ihrer Beschäftigten an eine bei der Deutschen Rentenversicherung eingerichtete zentrale Speicherstelle zu melden. Hierzu hatte der Bundesrat auf Initiative Niedersachsens zusammen mit zwei weiteren Ländern datenschutzrechtliche Bedenken vorgebracht, da nach dem Gesetzentwurf von allen abhängig Beschäftigten einkommensrelevante Daten gespeichert werden sollen, obwohl feststeht, dass diese Daten in vielen Einzelfällen tatsächlich nicht gebraucht werden. Dies widerspricht dem Grundsatz der Datensparsamkeit. Der Gesetzentwurf wurde trotz dieser Einwände, wenn auch mit weniger Datenbestandteilen als zunächst vorgesehen, verabschiedet. Gleichzeitig wurde das Bundesministerium für Arbeit und Soziales ermächtigt, durch Rechtsverordnung das Nähere zu Form, Inhalt und Verfahren für die Datenübermittlung zu regeln.

Der Entwurf der ELENA-Datensatzverordnung (BR-Drs. 892/09) wurde inzwischen vorgelegt und im Februar 2010 im Bundesrat behandelt. Der Bundesrat hat in seiner Stellungnahme zu dem Entwurf mit Unterstützung Niedersachsens nochmals auf die besondere datenschutzrechtliche und damit verfassungsrechtliche Brisanz des ELENA-Verfahrens hingewiesen, die sich bei dieser umfangreichen Datenspeicherung stellt. Diese Datenhaltung ist verfassungsrechtlich nur zulässig, wenn neben der grundsätzlichen Erforderlichkeit zum Zeitpunkt der Speicherung deren Zweck bestimmt ist und wirksame technische, organisatorische und rechtliche Sicherungen gegen Zweckänderungen und Datenmissbrauch gewährleistet sind. Insbesondere sind die gesetzlichen Vorgaben des § 97 Abs. 1 SGB IV zu beachten, wonach nur die Daten vom Arbeitgeber an die zentrale Speicherstelle zu melden sind, die für die Erstellung der Einkommensnachweise erforderlich sind. Weitere personenbezogene Daten darf die Meldung nicht enthalten.

Die Minimierung des Datensatzes liegt auch im Interesse der Wirtschaft. Der erhoffte Bürokratieabbau kann nur erreicht werden, wenn möglichst viele Bescheinigungen, die die Arbeitgeber bislang in Papierform erstellen, in das ELENA-Verfahren aufgenommen werden. Dies steht allerdings nicht in Widerspruch zu einem möglichst geringen Datenumfang, sondern ist eine Frage der sinnvollen Nutzung der ohnehin erhobenen und übermittelten Daten. Um den mit der Erhebung entstehenden Aufwand und die entlastende Wirkung durch den Wegfall des Ausstellens von Papierbescheinigungen in ein günstiges Verhältnis zu bringen, sollte die Bundesregierung zügig sämtliche Entgeltnachweise in das ELENA-Verfahren aufnehmen und den Entgeltbegriff im Zuge dessen harmonisieren.

Die Verordnung ist am 27.02.2010 in Kraft getreten.

Der Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD) und der Arbeitskreis Vorratsdatenspeicherung haben am 31.03.2010 beim Bundesverfassungsgericht (BVerfG) eine Verfassungsbeschwerde gegen das ELENA-Verfahrensgesetz eingelegt. Sie halten die Sammlung der hochsensiblen Daten für rechtswidrig. Dabei stützen sie sich auch auf das Urteil des BVerfG zur Vorratsdatenspeicherung, nach dem die Speicherung von Daten besonderen Einschränkungen unterliegt.

Der verlorene USB-Stick

Der vom LfD geschilderte Einzelfall wurde zum Anlass genommen, die Beschäftigten der Steuerfahndung nochmals auf die ordnungsgemäße Handhabung von Daten hinzuweisen und für den Umgang mit personenbezogenen Daten zu sensibilisieren. In der Finanzverwaltung wurde eine umfassende Sicherheitslösung initiiert, über deren Fortgang der LfD laufend informiert wird.

2. Datenschutz in der Wirtschaft

In diesem Abschnitt spricht der LfD insbesondere die Bereiche an, in denen seit einiger Zeit verstärkt Missbrauch mit personenbezogenen Daten aufgedeckt oder zumindest befürchtet wurde.

Überwachung der Beschäftigten im Lebensmitteldiscountbereich/Arbeitnehmerdatenschutz

Beschäftigte in Großunternehmen wurden in unangemessener Weise beobachtet und ihre personenbezogenen Daten erhoben. Insbesondere auf Anregung des Bundesrates wurde inzwischen eine Regelung zum Arbeitnehmerdatenschutz in das BDSG aufgenommen (§ 32 BDSG).

Bislang standen Beschäftigten, wie jeder anderen Person auch, lediglich allgemeine Interessenabwägungen gemäß § 28 BDSG zu. Die neue Regelung des § 32 BDSG konkretisiert die allgemeinen Grundsätze und soll dem besonderen Schutzbedürfnis von abhängig Beschäftigten Rechnung tragen. Grundsätzlich sollen personenbezogene Daten von Arbeitnehmerinnen und Arbeitnehmern für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet und genutzt werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Arbeitnehmerinnen und Arbeitnehmern nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die oder der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Die neue Regelung konkretisiert die von der Rechtsprechung erarbeiteten Grundsätze zum Beschäftigtendatenschutz und soll dem besonderen Schutzbedürfnis von abhängig Beschäftigten Rechnung tragen. Eine Arbeitsgruppe der Bundesressorts - unter Einbeziehung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - hat sich darüber hinaus mit umfassenderen Bestimmungen in diesem Bereich befasst (z. B. E-Mail-Verkehr, Internetnutzung, Videoüberwachung). Das Bundesministerium des Innern hat am 31.03.2010 Eckpunkte veröffentlicht, die in den Gesetzentwurf einfließen sollen. Es ist geplant, den Gesetzentwurf dem Bundeskabinett bis zur Sommerpause vorzulegen.

Google Street View

Mit der flächendeckenden Datenerfassung von digitalen Straßenansichten des Unternehmens Google (Google Street View) hat sich der Düsseldorfer Kreis (Abstimmungsgremium der obersten Datenschutzaufsichtsbehörden) intensiv befasst und auf eine auch aus Sicht der Landesregierung datenschutzrechtlich vertretbare Verfahrensweise verständigt, die die Zulässigkeitsvoraussetzungen für die Erstellung und Veröffentlichung digitaler Bildaufnahmen von Straßenpanoramen insbesondere im Internet definiert. Der LfD hat die Forderungen in seinem Bericht aufgeführt. Die konsequente Umsetzung dieser Zusagen wird von den Datenschutzbehörden kritisch beobachtet. Nach der Erfassung der Rohdaten plant Google die Onlinestellung der Daten für dieses Jahr.

Datenhandel

Beim Datenhandel führten bisher die Möglichkeiten der Weitergabe personenbezogener Daten ohne Einwilligung der betroffenen Person („Listenprivileg“, § 28 Abs. 3 Satz 1 Nr. 3 BDSG a. F.) verstärkt zu einer massenhaften und teilweise missbräuchlichen Datenübermittlung und -nutzung im Bereich der Privatwirtschaft. Die Regelung erlaubte, dass bestimmte personenbezogene Daten wie Name, Anschrift und Geburtsjahr, wenn sie listenmäßig oder in sonstiger Weise zusammengefasst sind, für Zwecke der Werbung oder der Markt- oder Meinungsforschung auch ohne Einwilligung der Betroffenen übermittelt und genutzt werden durften. Ein Verbot der Übermittlung und Nutzung bestand nur im Falle des Widerspruchs der Betroffenen, wobei von der Widerspruchsmöglichkeit kaum Gebrauch gemacht wurde.

Die insbesondere auf dem vom Bundesministerium des Innern einberufenen „Datenschutzgipfel“ am 04.09.2008 in Berlin formulierten Forderungen der Datenschützer nach einer vollständigen Abschaffung des Listenprivilegs beim Handel mit personenbezogenen Daten ohne Einwilligung konnten im Laufe des Verfahrens zur Änderung des BDSG im Jahr 2009 nicht vollständig durchgesetzt werden. Nach der Neufassung des § 28 BDSG ist für die Verarbeitung und Nutzung personenbezogener Daten zwar grundsätzlich eine Einwilligung des Betroffenen erforderlich; ohne ausdrückliche Einwilligung können die Daten aber weiterhin für eigene Werbezwecke oder für die eigene Markt- und Meinungsforschung, darüber hinaus für (Fremd-)Werbung gegenüber Freiberuflern oder Gewerbetätigen unter deren Geschäftsadresse oder auch für Zwecke der Spendenwerbung übermittelt und genutzt werden. Außerdem ist die Verarbeitung und Nutzung personenbezogener Daten nicht nur für Werbung gegenüber Freiberuflern und Gewerbetätigen unter deren Geschäftsadresse, sondern auch für Werbung generell „im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift“ (§ 28 Abs. 3 Satz 2 Nr. 2 BDSG n. F.) erlaubt. Nach § 28 Abs. 3 Satz 4 BDSG n. F. ist außerdem die Datenübermittlung an Dritte für Werbezwecke zulässig. In diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, eindeutig aus der Werbung hervorgehen. Das fehlende Einverständnis wird dabei durch ein Auskunftsrecht des Betroffenen ersetzt hinsichtlich der Herkunft der Daten und der Empfänger (§ 34 a Abs. 1 a BDSG n. F.). Damit sollen die Rechtmäßigkeit der Erhebung und nachfolgenden Verarbeitung der Daten geprüft werden können. Schließlich erlaubt § 28 Abs. 3 Satz 5 BDSG n. F. die Nutzung personenbezogener Daten für Werbezwecke für fremde Angebote, soweit für den Betroffenen bei der „Ansprache“ zum Zwecke der Werbung, etwa aus der Werbesendung, die für die Nutzung verantwortliche Stelle eindeutig erkennbar ist.

Die Landesregierung teilt die Auffassung des LfD, dass die Gesetzesänderungen aus dem vergangenen Jahr den Standard des Datenschutzes zwar verbessern, es aber darüber hinaus weiterhin notwendig ist, dass jede Bürgerin und jeder Bürger bei der Weitergabe der personenbezogenen Daten sorgfältig und umsichtig handelt und die zwingende Notwendigkeit dieser Weitergabe kritisch prüft und hinterfragt. Hier leisten sowohl der LfD als auch andere Stellen wie z. B. Schulen, Einrichtungen der Erwachsenenbildung und Verbraucherzentralen eine wichtige Aufklärungsarbeit.

3. Schwerpunktthema technisch-organisatorischer Datenschutz

Informationstechnik: Problemlöserin oder Werkzeug zur Kompromittierung?

Sowohl in der Landesverwaltung wie auch in allen weiteren öffentlichen und nicht öffentlichen Bereichen wird in zunehmendem Maß Informationstechnologie (IT) eingesetzt, um Geschäftsprozesse so effektiv wie möglich abzuwickeln. Dabei werden in erheblichem Ausmaß auch personenbezogene Daten verarbeitet, deren Schutz gewährleistet werden muss. Verschlüsselungsverfahren gehören bereits jetzt zu den technischen und organisatorischen Maßnahmen zur Zugangs- und Weitergabekontrolle, die im Rahmen des Schutzes personenbezogener Daten zu treffen sind. In § 9 BDSG - technische und organisatorische Maßnahmen - wird zu den Verschlüsselungsverfahren ausdrücklich auf den jeweiligen Stand der Technik abgestellt. Für Niedersachsen gibt § 7 NDSG vor, dass die Gestaltungsregeln dem Stand der Technik entsprechen müssen. Im Zuge der technischen Entwicklung, die nach Inkrafttreten der Regelung des § 7 NDSG rasant vorangeschritten ist, stellt sich die Frage, inwieweit diese Vorgaben angepasst werden müssen. Dies kann aber nicht isoliert für den Geltungsbereich des NDSG geschehen, sondern muss im Einklang mit dem BDSG und in Abstimmung auf Länderebene stehen.

Die vom LfD in seinem Tätigkeitsbericht aufgeführten Schutzziele sind dabei nur Teilaspekte und bereits in den Vorgaben des § 7 NDSG (auf Bundesebene § 9 BDSG nebst Anhang) und weiteren Regelungen dieser Gesetze enthalten. Eine Regelungslücke besteht daher derzeit nicht.

Identitätsmanagement und Verzeichnisdienst

Die zentrale Verwaltung der digitalen Identitäten der Landesbediensteten ist ein strategisches Ziel der Landesregierung. Dies hat zwar auch wirtschaftliche Hintergründe, da die aufwändige Pflege von mehreren Benutzerkonten für dieselbe natürliche Person entfällt. Vor allem bedeutet ein zentrales Identitätsmanagement (IDM) aber einen großen Gewinn an Sicherheit. Bei Austritten aus dem Landesdienst ist der Nutzer nur noch an einer Stelle zu deaktivieren, bei Um- und Versetzungen von Bediensteten wird der Gefahr der Anhäufung von Benutzerrechten wirksam entgegen gewirkt. Außerdem erhält man durch ein zentrales IDM auch ein einheitliches Verzeichnis aller Benutzer, welches gleichsam die nötigen (öffentlichen) Zertifikate enthalten kann.

Der IT-Bevollmächtigte der Landesregierung (CIO) wird in diesem Jahr ein solches IDM ausschreiben und für erste Verfahren zum Einsatz bringen. Der Erfolg wird allerdings - wie bei vielen übergreifenden IT-Verfahren in der Landesverwaltung - vor allem von der Akzeptanz der Verfahrensverantwortlichen abhängen.

Smartcards und Public key infrastrukture

Smartcards oder auf Smartcard-Chips basierende Tokens stellen sowohl für sich genommen (Verschlüsselung, Signaturfunktion) als auch im Kontext mit IDM einen wichtigen Baustein zur Verbesserung der Datensicherheit dar. Im Land werden derzeit etwa 12 000 solcher Signaturkarten eingesetzt, welche vor allem im Zusammenhang mit dem Haushaltswirtschaftssystem und dem Remote-Zugang zum Landesnetz eingesetzt werden. Aus Sicht der Landesregierung wäre es wünschenswert, wenn man mittelfristig eine möglichst flächendeckende Einführung erreichen könnte, da die Smartcard eine wichtige Middlewarekomponente darstellt, auf die weitere Dienste aufsetzen könnten. Smartcards in Verbindung mit einer Public-Key-Infrastruktur (PKI) stellen z. B. einen wesentlichen Baustein für eine im Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen (LSKN) bereits entwickelte verschlüsselte E-Mail-Kommunikation dar. Eine grundsätzliche Einführung dieser Technologie für jeden Landesbediensteten wäre zwar wünschenswert, ist allerdings auch mit nicht zu unterschätzendem Investitionsvolumen verbunden (je Signaturkarte Kosten in Höhe von rund 20 Euro pro Person pro Jahr, zuzüglich Einmalkosten für entsprechende Kartenleser an den PCs).

Ab 01.11.2010 soll in Deutschland der elektronische Personalausweis eingeführt werden, der neben dem elektronischen Identitätsnachweis auch die Möglichkeit einer sicheren, rechtsverbindlichen und signaturgesetzkonformen elektronischen Unterschrift bietet. Damit wird der Anwendungsbereich bei elektronischen Geschäften und Verfahren für Bürgerinnen und Bürger erheblich ausgeweitet.

Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität und Nachbesserungsbedarf bei Gesetzen

In seinem Urteil vom 27.02.2008 zur Online-Durchsuchung nach dem Nordrhein-westfälischen Verfassungsschutzgesetz hat das BVerfG die besondere Sensibilität und Eigenart der elektronischen Datenverarbeitung hervorgehoben und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Ausprägung des allgemeinen Persönlichkeitsrechts formuliert. Dem neuen Grundrecht kommt für die Entfaltung der Persönlichkeit eine erhebliche Bedeutung zu; die in informationstechnischen Systemen gespeicherten Daten können auch den Kernbereich privater Lebensgestaltung berühren.

Das BVerfG hat in seinem Urteil aber auch die hohe Bedeutung der Arbeit der Sicherheitsbehörden vor allem bei der Bekämpfung von Terrorismus und Organisierter Kriminalität anerkannt und den verdeckten Zugriff auf informationstechnische Systeme durch Online-Durchsuchung unter bestimmten Voraussetzungen für zulässig erachtet.

Eine Online-Durchsuchung kann nach dem Urteil nur zum Schutz höchster Rechtsgüter erfolgen. Eine konkrete Gefahr in dem Sinne, dass ein Schaden für diese Rechtsgüter bereits in absehbarer Zeit zu erwarten sein müsste - z. B. weil die Vorbereitung eines terroristischen Anschlags weit fort-

geschritten ist -, muss jedoch nicht vorliegen. Verdeckte Eingriffe in informationstechnische Systeme sind nach dem Urteil des BVerfG vielmehr schon dann gerechtfertigt, wenn ein bestimmtes Geschehen bereits so weit konkretisiert ist, dass die daran beteiligten Personen oder Personenkreise so bekannt sind, dass sie gezielt überwacht werden können.

Das BVerfG hat damit eine zwar hohe, den Bedürfnissen der Bekämpfung von Terrorismus und Organisierter Kriminalität jedoch Rechnung tragende Eingriffsschwelle formuliert. Es hat außerdem deutlich gemacht, dass auch die Unmöglichkeit, eine Erfassung von Daten aus dem unantastbaren Kernbereich privater Lebensgestaltung zu vermeiden, die Online-Durchsuchung nicht von vornherein unzulässig macht, solange für eine unverzügliche Aussonderung und Löschung kernbereichsrelevanter Inhalte gesorgt wird.

Die Vorgaben des BVerfG werden bei landesrechtlichen Regelungen der Online-Durchsuchung zu beachten sein. Insbesondere darf ein Zugriff auf informationstechnische Systeme nur gezielt bei bestimmten Personen oder fest umrissenen Personengruppen erfolgen, gegen die ein ausreichender Verdacht besteht. Dabei ist sicherzustellen, dass nicht auch Nutzer betroffen werden, gegen die ein solcher Verdacht nicht besteht. Angesichts der klaren Schranken und aufwändigen Schutzanforderungen, die das BVerfG verlangt hat, aber auch wegen des hohen technischen Aufwands, der mit jeder Online-Durchsuchung verbunden ist, soll und wird sich die Online-Durchsuchung nicht zu einem Standardverfahren der allgemeinen Kriminalitätsbekämpfung entwickeln.

Bei der Bekämpfung von Terrorismus und Organisierter Kriminalität kann die Online-Durchsuchung jedoch entscheidende Beiträge bringen und verhindern, dass durch die moderne Informationstechnologie ein geschützter Bereich entsteht, der dem staatlichen Zugriff vollständig entzogen ist und der von Kriminellen ungestört für ihre Planungen und Taten genutzt werden kann. Auch wenn jede Online-Durchsuchung mit technischen Schwierigkeiten verbunden ist und es gerade hoch organisierten und langfristig planenden Kriminellen immer wieder gelingen wird, sich solchen Maßnahmen zu entziehen, darf auf das Mittel der Online-Durchsuchung nicht verzichtet werden.

Das Gleiche gilt für die sogenannte Quellen-Telekommunikationsüberwachung, die z. B. für die Überwachung von verschlüsselter Internet-Telefonie benötigt wird. Nach Auffassung des BVerfG ist sie an der Telekommunikationsfreiheit aus Artikel 10 Grundgesetz zu messen, wenn technisch und rechtlich sichergestellt ist, dass ausschließlich auf Daten der laufenden Telekommunikation zugegriffen wird. Sie unterliegt daher auch nicht den gleichen Schranken wie die Online-Durchsuchung.

Aktiver Selbstdatenschutz

Um einen wirksamen Datenschutz zu erreichen, bedarf es - neben den rechtlichen Regelungen - technischer und organisatorischer Maßnahmen und einer umfassenden Datenschutzkompetenz jeder Bürgerin und jedes Bürgers. Jede Person muss dabei sorgfältig prüfen, ob, in welchem Umfang und wem sie ihre personenbezogenen Daten zur Kenntnis gibt. Nur im Zusammenspiel dieser Faktoren kann wirksamer Datenschutz gelingen. Die Vermittlung von Datenschutzkompetenz für einen aktiven Selbstdatenschutz ist eine gesamtgesellschaftliche Aufgabe, die vom Staat, insbesondere in Schule, Jugendarbeit und Jugendschutz, durch Erziehung in den Familien und von der Erwachsenenbildung bewältigt werden muss. Dies wird z. B. erreicht durch Informationen und Informationsangebote an jede Bürgerin und jeden Bürger, verbunden mit der Aufforderung, das individuelle Recht auf informationelle Selbstbestimmung und auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme konsequent zu verfolgen und gegenüber den Daten verarbeitenden Stellen geltend zu machen.

Gerade der Aufklärung Jugendlicher kommt dabei eine wesentliche Bedeutung zu (vgl. hierzu auch die Anmerkungen zur Medienkompetenz im Abschnitt zum öffentlichen Bereich). Es müssen Gefahrenpotenziale aufgezeigt werden und gleichzeitig Lösungen, wie der Missbrauch der Daten vermieden werden kann.

Die personelle und organisatorische Verstärkung des LfD nach dem Beschluss der Landesregierung vom 03.03.2009 soll auch dieser Aufgabe der Sensibilisierung der Bevölkerung im Umgang mit personenbezogenen Daten und der Wahrnehmung dieser Rechte zugute kommen.

Beteiligung bei IT-Verfahren des Landes und der Kommunen

Gemäß § 22 NDSG ist der LfD rechtzeitig über Planungen des Landes und der kommunalen Gebietskörperschaften zum Aufbau automatisierter Informationssysteme zu unterrichten. Dadurch soll dem LfD eine aktive Mitgestaltung im Vorfeld der Entwicklung und bei der Auswahl von Verfahren ermöglicht werden. Da gerade im Zuständigkeitsbereich des LSKN besonders viele neue Verfahren entwickelt werden, wurden hier wieder regelmäßige Gesprächsrunden zwischen dem LfD, dem LSKN und dem Chief Information Security Officer (CISO) initiiert.

IT-Sicherheit als Herausforderung für die Landesverwaltung

Das IT-Sicherheitsmanagement der Landesverwaltung ist zu systematisieren und zu professionalisieren. Der CISO hat inzwischen den Entwurf einer neuen Landesleitlinie erstellt, die die spezifischen Bedürfnisse der Ressorts besser aufnimmt und den Ressorts ermöglicht, sich und ihrem Geschäftsbereich eine angemessene Struktur für die Beteiligung an einem zentralen Informationssicherheitsmanagement zu geben. Der Landesrechnungshof hat die Leitlinie als erfolgversprechenden Ansatz bewertet. Die Beschlussfassung der Leitlinie ist für dieses Jahr vorgesehen.

Managed Storage

Der LfD wird durch die regelmäßigen Sitzungen des Koordinierungsausschusses IT über den Fortschritt des Projekts „Managed Storage“ informiert. Darüber hinaus bestehen Kontakte zwischen dem LSKN und dem LfD zu diesem Thema. Das im Tätigkeitsbericht monierte Sicherheits- und Datenschutzkonzept ist eine vertragliche Leistung des Outsourcing-Dienstleisters für das Projekt „Managed Storage“. Hier kam es zwar zu Verzögerungen, gleichwohl lag stets ein Konzept vor, welches lediglich einem längeren Qualitätssicherungsprozess unterzogen wurde. Weitere verfahrenspezifische Fragen des LfD hat der CIO inzwischen beantwortet.