Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz

Landesdatenschutzbeauftragter . Postfach 30 40 . 55020 Mainz

An den
Präsidenten des Landtags
Nordrhein-Westfalen
Postfach 10 11 43

40002 Düsseldorf

Ihr Zeichen:
Ihre Nachricht vom

Gesch.Z.: 2.9.01
(Bitte stets angeben !)

Tel.: 06131-208-2247

Datum: 14.01.2000

Öffentliche Anhörung des Ausschusses für Innere Verwaltung am 3.2.2000 zum Gesetz zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW)
Drucksache 12/4476

Sehr geehrter Herr Präsident,

für die Einladung zur Teilnahme an der öffentlichen Anhörung zur Änderung des nordrhein-westfälischen Datenschutzgesetzes danke ich Ihnen. Leider bin ich an diesem Tag dienstlich verhindert, so dass ich nicht persönlich erscheinen kann.

Gerne bin ich aber bereit, Ihnen aus meiner Sicht als langjährig (seit 1983) intensiv mit Datenschutz befasster Jurist und derzeitiger Landesbeauftragter für den Datenschutz Rheinland-Pfalz schriftlich meine Auffassung zu einigen nach meiner Ansicht bedeutsamen Gesichtspunkten in Bezug auf den vorgelegten Gesetzentwurf mitzuteilen.

Zum Zeitpunkt der beabsichtigten Novellierung

Es ist einerseits zu berücksichtigen, dass die Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-DSRL) bereits seit über 15 Monaten in nationales Recht hätte umgesetzt sein müssen. Andererseits ist aber auch darauf hinzuweisen, dass diese Umsetzung in erster Linie für den Bereich der Datenverarbeitung durch private Stellen Bedeutung hat, für die der Landesgesetzgeber nicht zuständig ist, und dass die Novellierung des dafür maßgeblichen Bundesdatenschutzgesetzes noch aussteht. Dies begründet für jeden bereits jetzt tätigen Landesgesetzgeber die missliche Situation, möglicherweise von Bundesregelungen abzuweichen und damit die Zersplitterung und Komplexität des Datenschutzrechtes zu verstärken, ohne dass dies sachlich unbedingt geboten wäre.

55116 Mainz • Deutschhausplatz 12 • Büro: Hintere Bleiche 34 – 38 • Tel.: 06131 – 208 2449 • Telefax: 06131 – 208 2497
E-Mail-Adresse: poststelle@datenschutz.rlp.de

Dieser Gesichtspunkt ist gerade auch für den Bereich bedeutsam, in dem der Landesgesetzgeber über eine Anpassung des Datenschutzrechts an die EG-DSRL hinausgeht und ergänzende Regelungen für neue Entwicklungen auf dem Gebiet der Informations- und Kommunikationstechnik schafft (Chipkartenregelung, Regelung der Video-Überwachung). In diesem Bereich ist es jedenfalls anzustreben und wünschenswert, möglichst einheitliche Anforderungen an die Datenverarbeitung von Bundes- und Landesbehörden zu formulieren.

Zu § 2 des Landesdatenschutzgesetzes:
Schon seit langem nimmt das nordrhein-westfälische Datenschutzgesetz neben dem Landtag, den Gerichten und dem Landesrechnungshof auch die Behörden der Staatsanwaltschaft, soweit sie strafverfolgend tätig werden, von den materiellen Datenschutzregelungen aus. Besonders im Hinblick auf die Auskunftsrechte der Betroffenen ist dies - da die Strafprozessordnung bislang insbesondere auch für die automatisierte Verarbeitung von Daten durch die Staatsanwaltschaften keine entsprechenden Regelungen vorsieht - nicht angemessen. Die Betroffenen haben hier aus meiner Sicht einen verfassungsrechtlichen Auskunftsanspruch gegenüber den Staatsanwaltschaften (selbstverständlich mit den Einschränkungen, die die Aufgabenerfüllung durch die Staatsanwaltschaften erfordert); dies lässt es aus meiner Sicht zumindest als angemessen erscheinen, einen entsprechenden Auskunftsanspruch auch im einfachen Gesetz zu normieren. Gleiches gilt für Löschungsansprüche der Betroffenen bei erwiesenermaßen unzutreffenden Datenspeicherungen.

Zur Einschränkung der Geltung des Landesdatenschutzgesetzes im Bereich der Gerichte halte ich den im nordrhein-westfälischen – wie auch im rheinland-pfälzischen – Landesdatenschutzgesetz verwandten Begriff der „Verwaltungsaufgaben der Gerichte" für ungeeignet. Dem Ziel des effektiven Grundrechtsschutzes unter Wahrung der Unabhängigkeit der Gerichte wäre es angemessener, nur den Bereich der gerichtlichen Tätigkeit aus dem Anwendungsbereich des Landesdatenschutzgesetzes auszunehmen, der der richterlichen Unabhängigkeit unterliegt. In diesem Sinn enthalten beispielsweise das berlinische und das schleswig-holsteinische Landesdatenschutzgesetz vorbildliche Regelungen; auch auf die Datenschutzgesetze Bremens und Hamburgs kann in diesem Zusammenhang verwiesen werden.

Zu § 4 Abs. 3 des Gesetzentwurfs:
Mit dieser Regelung soll bewirkt werden, dass die nach Artikel 8 der EG-DSRL als besonders sensibel angesehenen Daten besonders geschützt werden. Angesichts der in § 4 Abs. 3 Nrn. 1 - 4 aufgezählten zum Teil recht weit gehenden Durchbrechungsmöglichkeiten dieses Schutzes ist es aus meiner Sicht erforderlich, klarzustellen, dass diese datenschutzgesetzliche Regelung keinesfalls zu einer gegenüber dem bisher bestehenden Rechtszustand weiter gehenden Datenverarbeitungsbefugnis bezüglich dieser sensiblen Daten führt. Es sollte also etwa folgende Formulierung an § 4 Abs. 3 angefügt werden: „Sonstige Regelungen über die Geheimhaltung der in Satz 1 genannten Daten bleiben unberührt."

Es bestünde sonst die Gefahr, dass unter Berufung auf § 4 Abs. 3 Daten, die etwa durch das Arztgeheimnis oder - wie die Information über das religiöse Bekenntnis - durch Artikel

140 Grundgesetz i.V.m. Artikel 136 Weimarer Reichsverfassung geschützt sind, in weitergehendem Umfang als bisher erhoben, gespeichert oder übermittelt werden.

Zu § 10 Abs. 2 des Gesetzentwurfs:
Der Gesetzentwurf sieht vor, die bisherigen enumerativ aufgezählten Kontrollmaßnahmen (die sog. 10 Gebote des technischen und organisatorischen Datenschutzes) durch die Formulierung von sechs Maßnahmen des technischen und organisatorischen Datenschutzes zu ersetzen. Ich habe Zweifel, ob die gefundenen Formulierungen wirklich in jedem Fall praxistauglich sind und eine Verbesserung gegenüber den bisherigen Regelungen darstellen. So kann die „Unversehrtheit" von personenbezogenen Daten während der Verarbeitung (dies ist ein Bestandteil der „Integrität" der Daten gem. § 10 Abs. 2 Nr. 2 des Entwurfs) ganz sicher nicht gewährleistet werden, wenn die automatisierte Datenverarbeitung gerade darauf abzielt, Daten zu verändern, sie etwa zu aggregieren, im Rahmen von Berechnungen neue Ergebnisse zu erzielen und damit zu verändern u.ä.. Im Gesetzestext müßte also zumindest zum Ausdruck kommen, dass damit nicht befugte, sondern nur unbefugte Datenveränderungen ausgeschlossen werden sollen.

Die „Verfügbarkeit" von Daten im Sinne des § 10 Abs. 2 Nr. 3 des Gesetzentwurfs dürfte nur in seltenen Ausnahmefällen als Ziel des Datenschutzes im Sinne der Wahrung des informationellen Selbstbestimmungsrechtes der Betroffenen anzusehen sein. Im Regelfall ist dies ein Ziel, dessen Verfolgung im Interesse der Aufgabenwahrnehmung der datenverarbeitenden öffentlichen Stelle, nicht aber unbedingt im Interesse des betroffenen Bürgers liegt. Die Gewährleistung der Verfügbarkeit von Daten ist also nur in dem Umfang datenschutzrelevant, in dem die Datenverarbeitung dem Persönlichkeitsrecht der Betroffenen dient, etwa bei der Abgabe elektronischer Willenserklärungen u.ä. Auf diesen Bereich sollte sich der Geltungsanspruch des Datenschutzgesetzes auch in seinen Einzelanforderungen beschränken.

Die Regelung über die „Authentizität" von Daten (§ 10 Abs. 2 Nr. 4 des Entwurfs) ist aus meiner Sicht unklar: Was ist mit „Ursprung" von Daten gemeint? Dieser Begriff ist definitionsbedürftig. Die Anforderung dürfte insgesamt zudem nur in Bezug auf solche Daten angemessen sein, die eine besondere Relevanz (sei es unter dem Aspekt der Bedeutung für den Persönlichkeitsschutz oder für den Rechtsverkehr) besitzen. Ihre Ausweitung auf unterschiedslos alle personenbezogenen Daten dürfte in vielen Fällen einen sachlich nicht gerechtfertigten Aufwand verursachen.

Die Anforderung an die „Revisionsfähigkeit" gem. § 10 Abs. 2 Nr. 5 des Entwurfs ist zwar außerordentlich datenschutzfreundlich. Insofern begrüße ich sie dem Grunde nach. Allerdings wird damit eine umfassende ausnahmslose Protokollierungspflicht der datenverarbeitenden Stellen begründet. Eine solche Anforderung scheint mir nicht in jedem Fall - etwa im Fall der Verarbeitung von Bagatelldaten - begründet zu sein.

Aus dem Transparenzgebot des § 10 Abs. 2 Nr. 6 ergibt sich die Pflicht, Verfahren so einzurichten, dass sie in zumutbarer Zeit nachvollzogen werden können. Diese Pflicht sollte um die Anforderung erweitert werden, dass dies auch mit zumutbarem Aufwand möglich sein muß.

Insgesamt ist anzumerken, dass mit dieser Neuregelung eine Abkehr von der bisherigen Systematik im Bereich des technischen und organisatorischen Datenschutzes begründet wird, die länderübergreifende Aktivitäten bei der Datenverarbeitung erschweren könnte.

Zu § 10 Abs. 3 des Gesetzentwurfs:
In dieser Regelung wird gefordert, dass die datenverarbeitenden Stellen ein Sicherheitskonzept dokumentieren müssen, zu dessen Bestandteilen eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Grundrecht auf Datenschutz gehört.

Aus Datenschutzsicht ist es in vielen Fällen sicherlich gerechtfertigt, den datenverarbeitenden Stellen eine solche Prüfungspflicht aufzuerlegen; die EG-DSRL enthält zudem eine entsprechende Vorgabe, die allerdings auf besonders risikobehaftete Datenverarbeitungen beschränkt ist. Die Verpflichtung, in allen Fällen eine solche Vorabkontrolle durchzuführen und das Ergebnis einer solchen Vorabkontrolle in jedem Fall aufzuzeichnen, wird zu erheblichen Erschwerungen für die datenverarbeitenden Stellen (wobei auch an Stellen mit geringer Verwaltungskraft wie beispielsweise Schulen zu denken ist) führen. Aus meiner Sicht ist jedenfalls eine solche ausnahmslose Dokumentationspflicht angesichts der weiten Verbreitung der automatisierten Datenverarbeitung und der Tatsache, dass häufig auch unter dem Gesichtspunkt des Datenschutzes völlig unproblematische Verarbeitungen erfolgen, nicht angemessen und führt zu einer Bürokratisierung des Datenschutzes in einem nicht erforderlichen Umfang.

Zu § 12 Abs. 2 des Gesetzentwurfs:
In dieser Vorschrift wird vorgeschrieben, dass betroffene Personen bei Beginn der Speicherung oder im Fall einer vorgesehenen Übermittlung bei der ersten Übermittlung davon zu benachrichtigen sind, wenn Daten ohne ihre Kenntnis erstmals erhoben worden sind. Eingeschränkt wird diese Pflicht der datenverarbeitenden Stellen durch folgende Kriterien: Die entsprechende Benachrichtigung kann unterbleiben, wenn die Erfüllung der Aufgaben dadurch beeinträchtigt werden würde, wenn die betroffene Person auf andere Weise von der Speicherung oder Übermittlung Kenntnis erhält, wenn die Übermittlung durch Gesetz oder eine andere Rechtsvorschrift ausdrücklich vorgesehen ist oder wenn die Daten zu statistischen Zwecken verarbeitet werden und dies durch Gesetz oder eine andere Rechtsvorschrift vorgeschrieben ist.

Eine derartige umfassende Benachrichtigungspflicht scheint mir problematisch zu sein. Nach meiner Kenntnis gehen die Erfahrungen, die andere Länder mit entsprechenden Regelungen hatten, dahin, dass der Aufwand in keinem Verhältnis zum datenschutzrechtlichen Ertrag der Maßnahme steht. Ich erinnere mich in diesem Zusammenhang an eine vergleichbare Regelung im hessischen Datenschutzgesetz, die inzwischen auch förmlich entfallen ist, nachdem sie wegen mangelnder Praktikabilität nur selten befolgt worden ist. Aus meiner Sicht sollte deshalb der Gesichtspunkt des „unverhältnismäßigen Aufwands" als Schranke der Benachrichtigungspflicht, wie er auch in Art 11 Abs. 2 EG-DSRL Ausdruck gefunden hat, ebenfalls in das Gesetz aufgenommen werden.

Zu § 16 des Gesetzentwurfs:
Zunächst ist darauf hinzuweisen, dass die Kettenverweisungen in dieser Vorschrift (etwa von § 16 Abs. 1 Satz 2 des Entwurfs auf Satz 1 Buchst. b und von dort auf § 13 Abs. 2 Satz

1 Buchst. i) das Gesetz außerordentlich kompliziert machen. Aus meiner Sicht sollten derartige Kettenverweisungen durch Übernahme der jeweiligen Inhalte in die Ursprungsnorm aufgelöst werden.

Inhaltlich ist die Anhörungspflicht der von einer Übermittlung betroffenen Person in diesen Fällen aus datenschutzrechtlicher Sicht sicher zu begrüßen. In welchem Umfang dies zu Belastungen der Verwaltungspraxis und auch zu einer Ablehnung rechtmäßiger Übermittlungsersuchen betroffener Bürger und Stellen führt, deren Anliegen - zu Unrecht - aus Furcht vor der damit verbundenen arbeitsmäßigen Belastung durch die Anhörung der Betroffenen nicht entsprochen wird, ist allerdings nicht abzusehen. Entsprechende Tendenzen sind in der Praxis bereits jetzt auch ohne eine solche Anhörungspflicht nicht selten festzustellen.

Zu § 21 Abs. 3 des Landesdatenschutzgesetzes
Die Eingliederung des Landesbeauftragten für den Datenschutz in das Innenministerium unter Übertragung der Dienstaufsicht auf den Innenminister hat in der Praxis in der Vergangenheit - soweit ich dies beurteilen kann – nur ausnahmsweise (etwa in Baden-Württemberg; vgl. die Ausführungen der baden-württembergischen Landesbeauftragten für den Datenschutz anläßlich einer Anhörung des Landtags Rheinland-Pfalz zu dem Landesgesetz zur Bestellung eines Landesbeauftragten für den Datenschutz) zu Problemen geführt. Dennoch ist dies ein Modell, das aus meiner Sicht dem Ziel der Betonung der Unabhängigkeit des oder der Landesbeauftragten für den Datenschutz nicht entspricht. Deswegen geht die Tendenz in den Ländern dahin, den Landesbeauftragten für den Datenschutz als unabhängige oberste Landesbehörde zu konstituieren. Dies halte ich für die angemessenere Organisationsform.

Zu § 28 des Gesetzentwurfs:
Das Verhältnis von wissenschaftlicher Forschung und Datenschutz ist traditionell problematisch, da jedenfalls in wichtigen Teilbereichen der wissenschaftlichen Forschung die Erhebung personenbeziehbarer Daten erforderlich ist oder die Nutzung personenbezogener Daten die Erreichung des Forschungsziels jedenfalls erleichtert. In diesem Zusammenhang ist etwa an Verlaufsstudien im Bereich der Medizin oder an historische Forschungen der verschiedensten Art zu denken. Das Spannungsverhältnis zwischen dem Grundrecht auf Datenschutz der betroffenen Einzelpersonen einerseits und dem Grundrecht auf Wissenschaftsfreiheit andererseits ist komplex und nur schwer auflösbar.

§ 28 des Gesetzentwurfs scheint mir aber auch vor diesem Hintergrund eine zu starke staatliche Kontrolle über die wissenschaftlich Tätigen zu begründen. Sicher ist es angemessen, zu fordern, dass auch zu wissenschaftlichen Zwecken nur dann personenbezogene Daten verarbeitet werden dürfen, wenn dies zur Erreichung des angestrebten Zieles auch erforderlich ist. Für problematisch halte ich es allerdings, dies als von staatlichen Stellen überprüfbare allgemeine Rechtspflicht der wissenschaftlich Tätigen zu formulieren und auch die Fälle einer solchen Einschränkung und Prüfung zu unterwerfen, in denen die betroffenen Bürger auf der Basis der Freiwilligkeit ihr Einverständnis in die beabsichtigte Datenverarbeitung zu wissenschaftlichen Zwecken erteilen.

Folgendes tritt hinzu: Die in Abs. 1 enthaltene Sollvorschrift lässt Ausnahmen nur zu, wenn der Anonymisierung „wissenschaftliche Gründe" entgegenstehen. Ob Gründe der Effizienz in diesem Zusammenhang als wissenschaftliche Gründe anzusehen sind, ist offen. Effizienz ist aber auch für die Wissenschaft wichtig, sogar existenznotwendig.

Die Pseudonymisierung ist auch aus meiner Sicht eine taugliche Maßnahme des technischen Datenschutzes. Ich habe allerdings Zweifel, ob es mit der Wissenschaftsfreiheit vereinbar ist, wenn in diesem Zusammenhang gefordert wird, die mit der Forschung befassten Personen der Aufsicht der übermittelnden öffentlichen Stelle zu unterstellen.

Die Anforderungen des § 28 Abs. 1 bis 4 sollen unmittelbar nur für wissenschaftlich tätige öffentliche Stellen des Landes Nordrhein-Westfalen gelten. Dies ergibt sich aus Abs. 5 des Gesetzentwurfs. Ich halte es ebenfalls unter dem Gesichtspunkt der Wissenschaftsfreiheit für problematisch, den privaten forschungstreibenden Stellen Daten nur unter der Voraussetzung zur Verfügung zu stellen, dass sie sich der jederzeitigen Kontrolle durch den Landesbeauftragten für den Datenschutz unterwerfen.

Zu § 29 a des Gesetzentwurfs:
Mit dieser Regelung über den Chipkarteneinsatz betritt der nordrhein-westfälische Landesgesetzgeber Neuland. Grundsätzlich meine ich, dass sie geeignet ist, das informationelle Selbstbestimmungsrecht der Betroffenen auch in diesem Bereich zu schützen.

Zu § 29 b des Gesetzentwurfs:
Auch die Regelung der Videoüberwachung, die im Gesetzentwurf „optisch-elektronische Überwachung" genannt wird, hat bislang nur wenig Vorbilder. Die vorgesehene Regelung führt allerdings im Vergleich zur geltenden Rechtslage zu keiner wesentlichen Erhöhung des Schutzniveaus, es wird im Gegenteil durch das Abstellen auf die Dienlichkeit einer Maßnahme im Unterschied zum derzeit geltenden Erforderlichkeitsgrundsatz abgesenkt. Dies sollte geändert werden. Abgesehen davon halte ich die gesetzliche Regelung aber für geeignet, erste Erfahrungen zu gewinnen. Die damit geforderten begleitenden Maßnahmen beim Einsatz solcher Überwachungssysteme dürften nach meinem derzeitigen Kenntnisstand angemessen sein.

Es ist sicherlich entbehrlich, dass ich auf alle sonstigen aus meiner Sicht begrüßenswerten Neuregelungen des vorgelegten Entwurfs (wozu ich beispielsweise auch die Normierung des Grundsatzes der Datensparsamkeit und die Etablierung eines „Datenschutz-Audits" zähle) ausdrücklich und gesondert eingehe. Insgesamt halte ich ihn – von den oben erwähnten Punkten, die im Laufe des Gesetzgebungsverfahrens problemlos bereinigt werden könnten – für gelungen und geeignet, die Datenschutzdiskussion auch in den anderen Ländern positiv zu beeinflussen.

Mit freundlichen Grüßen

Prof. Dr. Walter Rudolf