Innenministerium des Landes Nordrhein-Westfalen

Innenministerium NRW, 40190 Düsseldorf

Haroldstraße 5,
40213 Düsseldorf

Telefon
(0211) 871 01
Durchwahl
(0211) 871 2599

Aktenzeichen
I A 5-1.2.11.2

An den
Präsidenten des Landtags
Nordrhein-Westfalen

40221 Düsseldorf

für den Ausschuss für Innere Verwaltung
und Verwaltungsstrukturreform (12o-fach) 19.01.2001

Betr.: 7. Bericht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden

Die Landesregierung hat am 12. Dezember 2000 den 7. Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden beschlossen. Die Berichterstattung erstreckt sich auf den Zeitraum vom 1. Januar 1999 bis zum 31. Mai 2000.

Dieser regelmäßig zu erstattende Bericht wurde bisher von der Landesregierung im Abstand von zwei Jahren dem Landtag vorgelegt. Rechtsgrundlage war § 27 des Datenschutzgesetzes Nordrhein-Westfalen in der bis zum 30. Mai 2000 geltenden Fassung. Die Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes (BDSG), über deren Tätigkeit berichtet wurde, waren die Bezirksregierungen Arnsberg und Köln.

Am 31. Mai 2000 sind die Änderungen des Datenschutzgesetzes Nordrhein-Westfalen in Kraft getreten. Das Gesetz bestimmt,

E-mail: poststelle@im.nrw.de Telefax (0211) 871 3355
Straßenbahnlinien 704, 709 und 719 bis Haltestelle Poststraße

nunmehr in § 22 Abs. 6, dass Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich nach § 38 BDSG die Landesbeauftragte für den Datenschutz ist.

Daraus folgt, dass die Landesbeauftragte für den Datenschutz künftig aufgrund der Neufassung des § 27 des Datenschutzgesetzes Nordrhein-Westfalen auch über ihre Tätigkeit als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich zu berichten hat. Da die Zuständigkeitsverlagerung in den vom Gesetz vorgeschriebenen Zwei-Jahres-Zeitraum fällt, endet der 7. Bericht der Landesregierung mit dem 31. Mai 2000. Für den Zeitraum vom 1. Juni 2000 bis zum 31. Dezember 2000 wird die Landesbeauftragte für den Datenschutz einen eigenen Bericht vorlegen.

Unter Bezugnahme auf § 27 des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) alter Fassung lege ich namens der Landesregierung den Bericht vor (in 300facher Ausfertigung).

(Dr. Fritz Behrens)

Datenschutz
im nicht-öffentlichen Bereich

Siebter Bericht

der Landesregierung Nordrhein-Westfalen

über die Tätigkeit der für den

Datenschutz im nicht-öffentlichen Bereich

zuständigen Aufsichtsbehörden

an den Landtag

Nordrhein-Westfalen

Berichtszeitraum
1. Januar 1999 bis 31. Mai 2000

G L I E D E R U N G

Einleitung

Der vorliegende siebte Bericht gibt einen Überblick über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden in Nordrhein-Westfalen. Die Berichterstattung erstreckt sich über den Zeitraum vom 1. Januar 1999 bis 31. Mai 2000.

Am 31. Mai 2000 ist das geänderte Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) in Kraft getreten. Das Gesetz sieht in § 22 Abs. 6 vor, dass Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich im Sinne des § 38 Bundesdatenschutzgesetz (BDSG) nunmehr der/die Landesbeauftragte für den Datenschutz ist. Örtliche Aufsichtsbehörden waren bisher die Bezirksregierung Arnsberg für die Regierungsbezirke Arnsberg, Detmold und Münster sowie die Bezirksregierung Köln für die Regierungsbezirke Düsseldorf und Köln. Oberste Aufsichtsbehörde ist nach wie vor das Innenministerium NRW.

Daraus folgt, dass die/der Landesbeauftragte für den Datenschutz künftig auch einen Tätigkeitsbericht über den Datenschutz im nicht-öffentlichen Bereich – erstmals beginnend ab 1. Juni 2000 – vorzulegen hat. Da die Zuständigkeitsverlagerung in den vom Gesetz vorgesehenen 2-Jahres-Zeitraum fällt, endet der siebte Bericht der Landesregierung mit dem 31. Mai 2000; für den Zeitraum vom 1. Juni 2000 bis 31. Dezember 2000 wird die Landesbeauftragte für den Datenschutz einen eigenen Bericht erstellen.

Der Datenschutz steht vor enormen Herausforderungen. Dies zeigt auch die Auswahl der in diesem Bericht dargestellten Themen. Das Fortschreiten der Informations- und Kommunikationstechnik eröffnet nahezu täglich neue Betätigungsfelder, wobei sich gerade im nicht-öffentlichen Bereich in immer vielfältigerer Weise Probleme des Datenschutzes ergeben. Der einzelne Bürger steht der wachsenden Technisierung seiner Umwelt in alltäglichen Bereich oft hilflos gegenüber. Mediendienste, Telebanking, online-Zugriffe von Banken und Versicherungen, Adresshändler und Chipkarten sind nur einige wenige Beispiele für die rasante Zunahme der Verbreitung, Nutzung und

Vernetzung von Informations- und Kommunikationstechnik. Die Gefahr eines möglichen Missbrauchs und der Zusammenführung von Daten zu vollständigen Persönlichkeitsprofilen nimmt angesichts dieser Entwicklung ständig zu. Die Vielfalt der Datenflüsse, die heute möglich sind, lässt erahnen, welche Wege und Aussichten der Medien- und Informationsgesellschaft von morgen eröffnet werden und welche Vorkehrungen zum Datenschutz und zur Datensicherheit zu treffen sind.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich werden daher im Rahmen ihrer Möglichkeiten noch stärker als bisher ihrem Beratungsauftrag nachkommen müssen. Der „Düsseldorfer Kreis", ein Beratungsgremium der obersten Datenschutz-Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich, dessen Vorsitz das Innenministerium Nordrhein-Westfalen führt, wird hierzu – wie schon in der Vergangenheit – seinen Beitrag leisten.

Von den Anfängen des Bundesdatenschutzgesetzes an ging es den Aufsichtsbehörden darum, soweit möglich mit den Wirtschaftsunternehmen gemeinsame Lösungen im Sinne eines wirksamen und praktikablen Datenschutzes auf hohem Niveau zu finden. Die regelmäßigen Treffen der Vertreter des „Düsseldorfer Kreises" sowie seiner Unter-Arbeitsgruppen mit Vertretern der Wirtschaft sind ein deutliches Zeichen für die gute Zusammenarbeit. Mögen die Bemühungen der zurückliegenden Jahre Grundlage und zugleich Ansporn dafür sein, Datenschutz und Datensicherheit auch weiterhin als gemeinsames Anliegen zu verstehen.

1. Übersicht über die Kontrolltätigkeit in Zahlen

Die Datenschutzaufsicht im nicht-öffentlichen Bereich lag bis zum 30.05.2000 bei der Bezirksregierung Arnsberg für die Regierungsbezirke Arnsberg, Detmold und Münster sowie bei der Bezirksregierung Köln für die Regierungsbezirke Düsseldorf und Köln. Ab 31.05.2000 ist die Landesbeauftragte für den Datenschutz Nordrhein-Westfalen für die Aufsicht neben dem öffentlichen auch für den nicht-öf-fentlichen Bereich zuständig.

1.1 Meldungen zum Register

Mit Stand 30.05.2000 waren zum Register der Aufsichtsbehörden folgende Stellen gemeldet:

a) Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Übermittlung speichern (§ 32 Abs. 1 Nr. 1 BDSG)

	Arnsberg	Köln
- Adresshandel, Direktmarketing	18	32
- Branchen- bzw. Kreditinformationsdienste (Wirtschaftsauskunfteien, SCHUFA, Warndienste)	39	56
Gesamt:	57	88

b) Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der anonymisierten Übermittlung speichern (§ 32 Abs. 1 Nr. 2 BDSG)

	Arnsberg	Köln
- Markt- und Meinungsforschungsinstitute	24	23

c) Stellen, die geschäftsmäßig personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen (§ 32 Abs. 1 Nr. 3 BDSG)

Arnsberg	Köln
526	757

In diesen Zahlen sind u. a. erfasst Service-Rechenzentren, Datenerfassungsbüros, Buchführungshelfer, Lettershops und Datenlöschungsunternehmen.

c) Gemeldete Unternehmen nach a) bis c) insgesamt

Arnsberg	Köln
607	868

Die Zahlen lassen erneut eine deutliche Zunahme erkennen. Der Anstieg der gemeldeten Stellen liegt wohl im Wesentlichen an der wachsenden Auslagerung von Geschäftsbereichen mit dem Schwerpunkt Datenverarbeitung auf spezialisierte Dienstleistungsunternehmen (Outsourcing), die dann als „Auftragsdatenverarbeiter" tätig werden.

1.2 Beschwerden

Von Januar 1999 bis Mai 2000 sind gegen datenverarbeitende Stellen, die Datenverarbeitung für **eigene** Zwecke (§ 28 BDSG) durchführten und für die eine Anlassaufsicht nach § 38 Abs. 1 BDSG bestand, bei der Bezirksregierung Arnsberg insgesamt 138 Beschwerden und bei der Bezirksregierung Köln 389 Beschwerden eingegangen.

Gegen Stellen, die geschäftsmäßig personenbezogene Daten für **fremde** Zwecke verarbeiteten (§ 32 Abs. 1 Nr. 1 bis 3 BDSG), wurden im vorgenannten Zeitraum bei der Bezirksregierung Arnsberg insgesamt 55 Beschwerden und bei der Bezirksregierung Köln 108 Beschwerden vorgebracht.

In diesen Zahlen sind – wie in den Vorjahren – sowohl Beschwerden von Betroffenen als auch Beschwerden von anderen Personen enthalten.

Die angegebenen Zahlen verteilen sich wie folgt:

Beschwerden gegen Stellen, die Datenverarbeitung für **eigene** Zwecke durchführen

	Arnsberg	Köln
- Handel / Handwerk	26	57
- Industrie / Großunternehmen	4	41
- Krankenhäuser, Ärzte, privatärztliche Verrechnungsstellen	16	31
- Kreditinstitute/-vermittler	5	75
- Versicherungen	18	72
- Vereine, Verbände	6	35
- Sonstige	63	78
Gesamt	138	389

Beschwerden gegen Stellen, die geschäftsmäßig personenbezogene Daten für **fremde** Zwecke verarbeiten

	Arnsberg	Köln
- Adresshandel, Direktmarketing	15	45
- Auskunfteien, Warndienste, SCHUFA	29	53
- Konzerndatenverarbeiter	2	--
- Markt- und Meinungsforschungs-institute	5	2
- Rechenzentren (Auftragsdatenver-arbeiter)	4	8
- Sonstige	--	--
Gesamt	55	108

Der Schwerpunkt der Beschwerden liegt mehr im Bereich der Datenverarbeitung für eigene Zwecke insbesondere in den Bereichen Handel / Handwerk, Kreditinstitute, Versicherungsunternehmen. Hier wirkt sich die wachsende Sensibilisierung der Bürgerinnen und Bürger für den Datenschutz aus, die sich in einer großen Anzahl von Anfragen und Beschwerden niederschlägt. Ebenso stand im Vordergrund vieler Beschwerden nach wie vor die Verarbeitung und Weitergabe von personenbezogenen Daten zu Werbezwekken (Marketing).
Beschwerden zu Datenverarbeitungen für fremde Zwecke betrafen schwerpunktmäßig unverändert die Tätigkeit von Auskunfteien (z. B. zur Zulässigkeit und Dauer der Speicherung von „Negativ"-Merkmalen).

Die geschäftsmäßige Verarbeitung personenbezogener Daten zu Werbezwekken hat vor allem infolge der zunehmenden Flut unerbetener Werbung zu vermehrten Anfragen und Beschwerden in Bezug auf Herkunft, Verarbeitung und Auswertung des Adressenmaterials und sonstiger Daten geführt.

Bei den insgesamt 690 Beschwerden kam es zu Beanstandungen oder Empfehlungen der Aufsichtsbehörden, denen im Wesentlichen entsprochen wurde. In den übrigen Fällen ergab sich kein Grund zu Beanstandungen; verein-

zelt wurden auch die Beschwerden aus verschiedenen Gründen (z. B. wegen Einstellung der Geschäftstätigkeit) nicht weiter verfolgt.

1.3 Anfragen und Beratungsersuchen

Die Aufsichtsbehörden erhielten wieder zahlreiche schriftliche Anfragen und Beratungsersuchen, die Datenverarbeitungen sowohl für eigene Zwecke (§ 28 BDSG) als auch für fremde Zwecke (§ 32 Abs. 1 BDSG) betrafen.

Die Unternehmen gehen – der Trend aus den Vorjahren setzt sich fort – verstärkt dazu über, bereits im Vorfeld von geplanten Datenverarbeitungsmaßnahmen die datenschutzrechtlichen Aspekte mit den Aufsichtsbehörden zu erörtern. Außerdem ist von einer wachsenden Sensibilität der Bürgerinnen und Bürger beim Umgang mit personenbezogenen Daten auszugehen.

1.4 Überprüfungen vor Ort

Diese Überprüfungen haben entweder im Rahmen der regelmäßigen Überwachung nach § 38 Abs. 2 BDSG bei Stellen mit Datenverarbeitung für fremde Zwecke (§ 32 Abs. 1 BDSG) oder aus konkretem Anlass, d. h. auf Grund von Beschwerden und sonstigen Hinweisen gem. § 38 Abs. 1 BDSG, stattgefunden.

	Arnsberg	Köln
a) Überprüfungen		
- Adresshandel / Direktmarketing	4	7
- Akten- und Datenvernichtungs-unternehmen	8	5
- Auskunfteien / SCHUFA	2	8
- Brancheninformationsdienste	--	1
- Buchführungshelfer / Schreibbüros	7	34
- Datenerfassungsbüros	4	20
- Markt- und Meinungsforschungsinstitute	--	5
- Mikroverfilmungsinstitute	4	5
- Rechenzentren (incl. Konzerndatenverarbeitung)	12	33
- Internetprovider	--	21
- Sonstige	1	---
Gesamt	42	139

	Arnsberg	Köln
b) konkrete Anlässe (§ 38 Abs. 1 BDSG) bei Stellen mit Datenverarbeitung		
für eigene Zwecke	1	55
für fremde Zwecke	-	25
Gesamt	1	80
Gesamt a) und b)	43	219

Auch im Rahmen der regelmäßigen Kontrolle bei Unternehmen, die geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeiten, wurden den technischen Prüfern immer wieder allgemeine Fragen zu datenschutzrechtlichen Problemen vorgetragen, die nicht in unmittelbarem Zusammenhang mit der Routineüberprüfung standen. Diese nicht gesondert erfassten Anfragen und die entsprechenden Beratungen und Empfehlungen sind in den o. g. Zahlen nicht enthalten.

Wie in den Vorjahren betrafen die Überprüfungen vor Ort technische Fragen der Datensicherheit und organisatorische Schutzvorkehrungen.

2. Stand der Novellierung des Bundesdatenschutzgesetzes (BDSG)

Gemäß der Europäischen Datenschutzrichtlinie 95/46 EG vom 24. Oktober 1995 waren die EG-Mitgliedstaaten und damit auch die Bundesrepublik Deutschland, aber auch die einzelnen Länder verpflichtet, innerhalb von drei Jahren die Umsetzung der Richtlinie durchzuführen. Die Richtlinie sieht eine Erweiterung der Informationsrechte der Bürgerinnen und Bürger vor und verpflichtet alle Mitgliedstaaten – ungeachtet des Spielraums, innerhalb dessen sie unter Beachtung des Gemeinschaftsrechts unterschiedliche nationale Regelungen treffen können – auf ein im Wesentlichen einheitliches Datenschutzniveau. Nachdem es der ehemaligen Bundesregierung nicht gelungen war, die Anpassung innerhalb der Drei-Jahres-Frist vorzunehmen, vereinbarte die neue Regierungskoalition im Oktober 1998, die notwendige Novellierung des BDSG kurzfristig durchzuführen. Wegen des Fristablaufs wurde entschieden, das BDSG in zwei Phasen zu novellieren: In der ersten Phase beschränkt sich die Novellierung vor allem auf die Umsetzung der EG-Datenschutzrichtlinie; in einer zweiten Phase soll dann das gesamte Datenschutzrecht umfassend modernisiert werden.

Seit 1995 haben die Länder die Novellierung begleitet und wiederholt zahlreiche Empfehlungen und Anregungen gegeben. Der von der Bundesregierung im Sommer 2000 vorgelegte Gesetzentwurf berücksichtigt – im Gegensatz zu seinen zahlreichen Vorgängern – eine Vielzahl dieser Vorschläge. Dennoch kann er nur als erster Schritt im Rahmen einer grundlegenden Überarbeitung und Weiterentwicklung des bestehenden Datenschutzrechts gesehen werden. Im Hinblick auf den Zeitdruck haben die Länder die Novellierung in zwei Phasen akzeptiert, ihre grundsätzlichen Bedenken gegen den schwer lesbaren Entwurf zurückgestellt und ihre Änderungsanträge im Gesetzgebungsverfahren auf das Notwendigste beschränkt.

Angesichts der Bedeutung des Datenschutzes als Qualitätsmerkmal für Anwendungen der neuen Informations- und Kommunikationstechniken ist es jedoch dringend geboten, in der zweiten Stufe der Novellierung ein transparentes und für die Praxis handhabbares Datenschutzrecht zu schaffen. Die

von der EG-Datenschutzrichtlinie eröffneten Gestaltungsspielräume können hierbei genutzt werden, um die Eigenverantwortlichkeit der datenverarbeitenden Stellen zu stärken und sicherzustellen, dass auch kleinere Unternehmen und Betriebe in der Lage sind, die Datenschutzbestimmungen effektiv umzusetzen. Hierzu gehört auch die Beibehaltung der Unterscheidung zwischen Vorschriften für den öffentlichen und den nicht-öffentlichen Bereich.

Die Länder werden auch im weiteren Verfahren ihre Vorstellungen, die sich u. a. aus der praktischen Aufsichtstätigkeit ergeben und im „Düsseldorfer Kreis" diskutiert werden, einbringen.

Angesichts der Zeitverzögerung durch die ehemalige Bundesregierung haben sich einige Länder – so auch Nordrhein-Westfalen - entschieden, die Novellierung ihrer jeweiligen Datenschutzgesetze unabhängig von der Änderung des BDSG durchzuführen. In Nordrhein-Westfalen ist das neue Datenschutzgesetz (DSG NRW) am 31. Mai 2000 in Kraft getreten.

3. Scoring-Verfahren bei der SCHUFA

Auch im Berichtszeitraum gab es wieder zahlreiche Anfragen bei den Aufsichtsbehörden über die Interpretation von Score-Werten bzw. bei der Einholung von Selbstauskünften.

Scoring-Verfahren erstellen mit statistisch mathematischen Methoden Prognosen über das zukünftige Verhalten von Personengruppen und drücken die Prognose in einer Punktzahl (Score) aus. Dabei handelt es sich um eine anonymisierte Auswertung aller im SCHUFA-Datenbestand gespeicherten Daten, auf deren Grundlage eine Wahrscheinlichkeit des Eintretens von Risiken prognostiziert wird, die z. B. mit einer Kontoeröffnung oder der Einräumung eines Kredites verbunden sind. Diese Wahrscheinlichkeitsaussage gilt nicht für ein konkrete Person, sondern nur für Gruppen von Personen mit gleichem Datenprofil. Auf Grund der Auswertung einer Vielzahl gleichartiger Datensätze soll es möglich sein, vorherzusagen, dass ein Kreditverhältnis ähnlich verlaufen wird, wie in der Vergangenheit die Kreditverhältnisse der herangezogenen Vergleichspersonen. Weder die SCHUFA noch der SCHUFA-Anschlusspartner (Abfrager) gibt den Betroffenen in der Regel Auskunft über die Höhe des Score-Wertes. Die SCHUFA begründet dies damit, dass der Score-Wert eine wechselnde Größe sei und bei ihr nicht gespeichert werde, welcher Score-Wert den Betroffenen im Zeitpunkt der Abfrage durch den Anschlusspartner zugeordnet wurde.

Die SCHUFA hielt zunächst die Durchführung des Scoring-Verfahrens durch die von den betroffenen Kunden unterzeichnete allgemeine Einwilligungsklausel für rechtlich abgedeckt, auch ohne dass das Scoring-Verfahren ausdrücklich darin erwähnt wird. In Verhandlungen des „Düsseldorfer Kreises“ mit der SCHUFA wurde inzwischen eine bessere Transparenz des Verfahrens für die Betroffenen erreicht. Bei der bevorstehenden Weiterentwicklung und Modernisierung der „SCHUFA-Klausel“ wird nunmehr in diese auch eine Information über das Scoring-Verfahren aufgenommen. Weitere Informationen sollen einem Merkblatt zu entnehmen sein, dass den Kunden der SCHUFA-Anschlusspartner von diesen auf Verlangen ausgehändigt wird. Damit erhält

der Betroffene eine Vorstellung davon, wie der Score-Wert zustande kommt. Das Merkblatt mit Hintergrundinformationen muss daher zumindest allgemeine Angaben über die Kriterien (Faktoren) des Score-Wertes enthalten. Der Betroffene muss darüber hinaus auch in jedem Fall beim angeschlossenem Unternehmen Auskunft über den Score-Wert erhalten, der bei der Kreditentscheidung berücksichtigt worden ist, damit er seinen Standpunkt geltend machen kann.

Die Forderungen der Aufsichtsbehörden sind derzeit noch Gesprächsthema mit der Kreditwirtschaft und der SCHUFA.

Ein weiteres Problem, das an die Aufsichtsbehörden herangetragen wurde, ist die SCHUFA-Selbstauskunft mit der Folge, dass der Betroffene einen negativen Score-Wert erhält.

Grundsätzlich hat jeder einen Anspruch darauf, zu erfahren, welche Daten über ihn gespeichert sind, ohne dass sich dies negativ für ihn auswirken darf. Die SCHUFA begründet ihr Verfahren damit, dass SCHUFA-Selbstauskünfte vermehrt von Personen abgefragt werden, bei denen eine Wahrscheinlichkeit des Eintretens eines Risikos gegeben sei. Daher habe eine solche Anfrage Auswirkungen auf die Höhe des Score-Wertes.

Die Aufsichtsbehörden sind auch zu diesem Thema noch in einer intensiven Diskussion mit der SCHUFA.

4. Verschmelzung von Unternehmen (Fusion)

Im Berichtszeitraum wurden zahlreiche Anfragen an die Aufsichtsbehörden gerichtet, die sich mit der datenschutzrechtlichen Problematik von Verschmelzungen im Sinne des § 2 Umwandlungsgesetz (UmwG) befassten.

Fusionen im Sinne dieses Gesetzes bzw. die Registereintragungen bewirken nach § 20 UmwG eine Gesamtrechtsnachfolge. Fraglich ist, ob hier eine Datenübermittlung im Sinne des § 3
Abs.5 Nr. 3 Bundesdatenschutzgesetz (BDSG) vorliegt. Dies wäre nur dann der Fall, wenn der Umwandlungsvertrag in Verbindung mit der beantragten und erfolgten Registereintragung als eine solche Übermittlung zu bewerten wäre. Dagegen spricht, dass der Vorgang der Fusion – sei es bei einer Fusion durch Neugründung oder bei einer Fusion durch Aufnahme – nicht dadurch gekennzeichnet ist, dass Daten vom Vertragspartner des Kunden an einem „Dritten" im Sinne des § 3 Abs. 9 BDSG gelangen, sondern dass sich die rechtliche Identität des Vertragspartners ändert.

Unter welchen Voraussetzungen Änderungen der rechtlichen Identität von Unternehmen und damit auf Grund der Gesamtrechtsnachfolge ein Wechsel bzw. eine Veränderung des Vertragspartners zulässig sind, ist eine Frage, die nicht vom BDSG zu beantworten ist. Dieses Gesetz regelt nur, dass sich sowohl vor als auch nach der Umwandlung die Datenverarbeitung etwa eines Kreditinstituts nach § 28 BDSG richten muss. Das BDSG ist nur maßgeblich für die Datenverarbeitung durch das „neue" Unternehmen.

Darüber hinaus lässt sich die datenschutzrechtliche Irrelevanz von Fusionen auch aus § 132 UmwG ableiten: Dort hat der Gesetzgeber die Gestaltungsfreiheit für den Abschluss von Umwandlungsverträgen durch die Bezugnahme auf Normen außerhalb des Umwandlungsgesetzes begrenzt. Dies hat er jedoch nur für ganz spezielle Umwandlungsarten getan. Unabhängig davon, ob das BDSG tatsächlich zu den nach § 132 UmwG zu beachtenden Schranken gehört, führt zumindest der Umkehrschluss dazu, dass das BDSG jedenfalls beim Abschluss und Vollzug sonstiger Umwandlungsverträ-

ge unbeachtlich sein muss. Im Ergebnis ist daher das BDSG für die Fusion von Unternehmen nicht anwendbar.

5. Videoüberwachung

Die Videoüberwachung in Geschäften und Banken sowie in Bahnhöfen, Parkhäusern, Taxis und Tankstellen nimmt, vor allem auch durch die Entwicklung neuartiger und preiswerterer Technik, ständig zu. Damit verbunden sind auch rechtliche Probleme. Durch eine Videoüberwachung wird in das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz) des davon betroffenen Personenkreises eingegriffen. Dieses Recht ist gegen das Interesse desjenigen, der die Videoüberwachung vornehmen will, abzuwägen. Es geraten nicht nur unbescholtene Personen in das Visier der Videoüberwachung, sondern es fallen dabei auch immense Mengen von Daten an. Die Zusammenführung dieser Daten mit weiteren Daten kann zu einem perfekten Bewegungsprofil einer betroffenen Person verdichtet werden.

Es besteht daher ein dringender datenschutzrechtlicher Regelungsbedarf über die Zulässigkeit der Videoüberwachung. Für den öffentlichen Bereich ist in Nordrhein-Westfalen im neuen Datenschutzgesetz (DSG NRW) eine gesetzliche Grundlage geschaffen worden (§ 29 b DSG NRW).

Für den nicht-öffentlichen Bereich sieht der Bundesgesetzgeber nunmehr in seinem Entwurf des neuen Bundesdatenschutzgesetzes ebenfalls eine Vorschrift (§ 6 b BDSG neu) vor, die die Zulässigkeit der Videoüberwachung öffentlich zugänglicher Räume ausdrücklich regelt.

Von der Regelung erfasst werden öffentlich zugängliche Räume, wie etwa Ausstellungsräume von Museen, Verkaufsräume, Schalterhallen u. ä. Nicht öffentlich zugängliche Räume, etwa Aufenthalts- und Sozialräume für Personal oder auch verwaltungsinterne Räumlichkeiten sind nicht Gegenstand der Regelung.

Insgesamt ist die neue Vorschrift zu begrüßen, da sie das Persönlichkeitsrecht der von der Videoüberwachung betroffenen Personen berücksichtigt, wenn auch in nicht ganz zufriedenstellender Weise. So geht die vorgesehene

Zulässigkeit der Videoüberwachung praktisch für jede Art der Aufgabenerfüllung zu weit. Hier wäre es wünschenswert, eine solche Maßnahme nur zum Schutz eigener wichtiger Interessen zuzulassen.

6. Mithören und Aufzeichnen von Telefongesprächen in Call-Centern

Auf Grund zahlreicher Anfragen im Berichtszeitraum befassten sich die Aufsichtsbehörden mit der Frage der Zulässigkeit des Mithörens und Aufzeichnens von geschäftlichen Telefongesprächen zwischen Mitarbeitern und Kunden.

Das Aufzeichnen von Telefongesprächen ist strafbar, soweit dies unbefugt im Sinne des § 201 Abs. 1 Strafgesetzbuch (StGB) erfolgt. Danach wird das unbefugte Aufnehmen des nicht-öffentlich gesprochenen Wortes eines anderen auf einem Tonträger mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe geahndet. Eine Befugnis zum Aufzeichnen von Telefongesprächen durch das Call-Center besteht nur dann, wenn die jeweiligen Gesprächsteilnehmer, also die Kunden und die Mitarbeiter, hierin eingewilligt haben oder eine gesetzliche Ermächtigung vorliegt.

Es würde nicht ausreichen, etwa im Zusammenhang mit der Veröffentlichung der Service-Telefonnummern etwaige Kunden auf die Aufzeichnung eingehender Kundengespräche hinzuweisen, da dies nicht als wirksame Einwilligung durch den Kunden gewertet werden kann. Auch eine vertragliche Einwilligungserklärung der Mitarbeiter wäre unwirksam, weil die Einwilligung offensichtlich auf Grund des Abhängigkeitsverhältnisses der Mitarbeiter zu ihrem Arbeitgeber unter faktischem Zwang und demnach nicht freiwillig erteilt würde.

Etwas anderes ergibt sich beim Mithören von Telefongesprächen. Gemäß § 201 Abs. 2 Satz 1 StGB wird zwar bestraft, wer unbefugt das nicht zu seiner Kenntnis bestimmte nicht-öffentliche Wort eines anderen mit einem Abhörgerät aufzeichnet. Allerdings liegt nach der Rechtsprechung ein strafbares Abhören nicht vor, soweit es sich nur um Mithöreinrichtungen handelt. Da in den Call-Centern offensichtlich nur Mithöreinrichtungen eingesetzt werden, ist das Mithören von Telefongesprächen zwar möglich, aber nur, soweit dies zur Wahrung der berechtigten Interessen des Arbeitgebers sowie im Rahmen der Zweckbestimmung der Arbeitsvertragsverhältnisse erforderlich

ist und kein Grund zu der Annahme besteht, dass dadurch schutzwürdige Interessen der Kunden oder Mitarbeiter beeinträchtigt werden.

Im Hinblick auf den Datenschutz gegenüber dem Kunden ist zu beachten, dass ein Kundengespräch unter Umständen zwischen den Gesprächspartnern eine persönliche Note erhalten kann. Deshalb ist es wichtig, dass der Kunde über das Mithören einer weiteren Person etwa durch vorherige Ansage unterrichtet wird.

7. Bonitätsprüfung vor (zahn)ärztlicher Behandlung

Die privatärztlichen Verrechnungsstellen sowie Ärzte und Zahnärzte sind zunehmend daran interessiert, die Bonität der von ihnen zu behandelnden Patienten durch entsprechende Anfragen bei einem Kreditschutzunternehmen oder einer Auskunftei überprüfen zu können. Dieses Interesse wird damit begründet, dass bei umfangreichen ärztlichen und zahnärztlichen Behandlungen finanzielle Vorleistungen erforderlich werden können, die mit einem erheblichen Risiko, nämlich der mangelnden Zahlungsfähigkeit des Patienten, verbunden sind. Das Risiko kann sowohl bei privatärztlichen Verrechnungsstellen, an die eine ärztliche Honorarforderung zum Einzug abgetreten wurde, als auch bei Ärzten, die mit ihren Patienten selbst abrechnen, entstehen.

Datenschutzrechtlich problematisch ist insbesondere, dass der anfragende Arzt seinen Patienten gegenüber dem Kreditschutzunternehmen oder der Auskunftei eindeutig identifizieren muss, bevor er die gewünschte Auskunft erhalten kann. Durch die Übermittlung der zur Identifikation benötigten Angaben wird aber zugleich offenbart, dass sich der Betroffene bei einem bestimmten Arzt in ärztlicher Behandlung befindet. Es werden somit besonders sensible Daten weitergegeben, die nach § 203 Strafgesetzbuch (StGB) der ärztlichen Schweigepflicht unterliegen.

Die Übermittlung von Patientendaten ist ohne Wissen und Einwilligung des Betroffenen nicht zulässig. Die ärztliche Schweigepflicht darf nur durchbrochen werden, wenn der Patient vorher über die beabsichtigte Weitergabe seiner Daten informiert worden ist und er in sie ausdrücklich schriftlich eingewilligt hat. In dem Fall, in dem die ärztliche Honorarforderung an eine privatärztliche Verrechnungsstelle abgetreten wurde, kann dies zusammen mit der Erklärung, mit der der Patient in die Übermittlung seiner Daten an die Verrechnungsstelle einwilligt, geschehen. Rechnet der Arzt mit dem Patienten selbst ab, so könnte die auch in diesem Fall erforderliche schriftliche Einwilligung in Verbindung mit einem Kostenvoranschlag für die Behandlung eingeholt werden.

In diesem Sinne haben sich auch die Mitglieder des „Düsseldorfer Kreises“ verständigt.

8. Datenverarbeitung durch privatärztliche Verrechnungsstellen

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vertreten mehrheitlich den Standpunkt, dass es sich bei der Datenübermittlung durch e-mail, z.B. von medizinischen Daten an privatärztliche Verrechnungsstellen, um Datenverarbeitung im Auftrag handelt, die einer Einwilligung der Betroffenen bedarf.

Dagegen vertreten der für die datenschutzrechtliche Aufsicht über die Postdienste zuständige Bundesbeauftragte für den Datenschutz und die zuständigen Bundesressorts den Standpunkt, dass es sich bei dem elektronischen Briefservice e-mail um eine reine Postdienstleistung handelt, bei deren Durchführung das bereichsspezifische Postrecht und damit auch das Postgeheimnis gilt und daher eine nach dem Datenschutzrecht notwendige Einwilligung nicht erforderlich ist.

Für den Fall, dass letztere Auffassung weiterhin bestritten wird, denken die Bundesressorts an eine gesetzliche Klarstellung.

9. Elektronisches Ticket im Verkehrsverbund Rhein-Ruhr (VRR)

Der Verkehrsverbund Rhein-Ruhr (VRR) plant den Einsatz eines elektronischen Fahrscheins.

Es ist vorgesehen, dass Fahrgäste die für die Fahrtkostenberechnung erforderlichen Daten mittels einer Chipkarte (EC-Karte) zur Verfügung stellen.

In der ersten Stufe der Einführung des neuen Systems sollen nur Vertragskunden eine vorbereitete Chipkarte erhalten. Eine solche Chipkarte ist vom Fahrgast beim Betreten des Busses in ein dafür vorgesehenes Lesegerät zu stecken. Eine Abrechnung der Fahrtkosten erfolgt dann auf Grund der auf der Chipkarte enthaltenen Daten. Ferner erfolgt ein Datenabgleich mit einer sogenannten Sperrdatei, in der Angaben über verlorengegangene, gestohlene oder illegal erstellte Chipkarten erfasst sind.

Das Zielsystem soll ab dem Jahr 2003 eingeführt werden. Hierbei sollen die Fahrgäste des VRR die für die Fahrtkostenberechnung erforderlichen Daten mittels einer Chipkarte kontaktlos zur Verfügung stellen. Der Fahrgast muss die Chipkarte nur bei sich tragen und nicht durch ein spezielles Gerät führen. Im Bereich der Türen der Busse sind sogenannte Chipkartenleser, die die Fahrstrecke durch Ein- und Ausstieg der Fahrgäste erfassen. Anschließend erfolgt eine monatliche Rechnungslegung. Der Datentransfer zwischen dem Rechner im Bus und der zentralen Datenbank erfolgt bei Rückkehr des Busses in den Betriebshof mittels einer kurzen Richtfunkstrecke.

Welche personenbezogenen Daten im Einzelnen erfasst und gespeichert werden, ist noch mit der zuständigen Aufsichtsbehörde abzustimmen. Dabei ist auch zu klären, wie lange die erfassten Bewegungsprofile aufgezeichnet bleiben dürfen.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich sind sich darüber einig, dass bei diesen Vorhaben folgenden datenschutzrechtlichen Erfordernissen Rechnung getragen werden muss:

- Zweckbindung
- Schutz des Persönlichkeitsrechts
- Recht auf informationelle Selbstbestimmung

Die Erhebung und Speicherung der personenbezogenen Daten sollen nur im notwendigen Umfang unter möglichst anonymer Handhabung erfolgen. Für die Abrechnung sollen nur die notwendigen Daten auf Vertragsbasis erhoben und verarbeitet werden.

Die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich werden sich mit den Zentralen Verkehrsverbänden ins Benehmen setzen und diese Probleme erörtern.

Elektronische Geldbörse („GeldKarte")

Die elektronische Geldbörse ist aus dem täglichen Geschäftsleben nicht mehr wegzudenken.

Die von den Banken ausgegebene EC-Karte ist mit einem Multifunktionschip ausgerüstet und an ein Girokonto gebunden. Sie wird an einem Ladeterminal mit einem Geldbetrag aufgeladen, der von dem Girokonto abgebucht wird. Der Vorgang des Ladens wird mit Kartendaten, Betrag und Datum bei einer sog. Karten-Evidenzzentrale (KEZ) des zuständigen Spitzenverbandes der Kreditwirtschaft gespeichert. Die GeldKarte kann zum bargeldlosen Einkauf bei Händlern benutzt werden, die dem Verfahren angeschlossen sind. Die Zahlung erfolgt dann durch Abbuchung des Kaufbetrages von der GeldKarte in einem Händlerterminal. Die Transaktionsdaten des Händlers werden an eine sog. Händler-Evidenzzentrale (HEZ) übermittelt, die ihrerseits die aufbereiteten Daten an die zuständige KEZ weiterleitet, sie aber auch selbst bis zu einer Zeitdauer von sieben Jahren speichert und die übermittelten Daten mit den bei ihr gespeicherten Daten der GeldKarte zusammenführt.

Die eigentliche Zahlungsabwicklung und Buchung erfolgt – mit Hilfe der Datenverarbeitung bei den Evidenzzentralen – über die Konten des Händlers bzw. des Käufers bei ihrer jeweiligen Bank. Bei den Evidenzzentralen entstehen sogenannte Schattenkonten, auf denen sich im Laufe der Zeit eine Vielzahl von Daten über das Kaufverhalten der einzelnen Karteninhaber ansammeln kann. Solche Daten könnten z.B. für die Direktwerbung dritter Unternehmen von erheblichem Interesse sein. Die Schattenkonten werden zwar nur anhand der EC-Kartennnummer geführt und enthalten weder Namen noch Anschriften der Karteninhaber; könnten jedoch mit Hilfe der bei den Banken gespeicherten Kundendaten identifiziert werden.

Die Problematik einer solchen Datenzusammenführung und z.B. auch

- der Datenarchivierung (Beschränkung auf die rechtlich und tatsächlich erforderliche Mindestdauer),
- der Auskunftsrechte,
- der Widerspruchsrechte,
- der Unterrichtungspflichten sowie
- der Datenverantwortlichkeit

wurden eingehend mit dem Zentralverband der Kreditindustrie, dem Zentralen Kreditausschuss – ZKA, erörtert. Nach intensiven Verhandlungen stehen nunmehr die obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich kurz davor, einvernehmlich mit dem ZKA datenschutzrechtliche Grundsätze hierzu festzulegen. Diese Grundsätze sollen dann vom ZKA den angeschlossenen Kreditinstituten zur Anwendung empfohlen werden.

Die technische Leistungsfähigkeit der Chipkarte ermöglicht über die Nutzung als GeldKarte hinaus vielfältige Zusatzanwendungen; z.B. als elektronischer Fahrausweis oder Telefonkarte. Hier sollte verhindert werden, dass über das unabdingbar notwendige Maß hinaus Datenspuren gelegt werden. Besonders wichtig ist in diesem Zusammenhang, dass die einzelnen Funktionen der Karte getrennt bleiben und ihre Vermischung durch technische Maßnahmen verhindert wird.

Sowohl bei der GeldKarte als auch bei ihren möglichen Zusatzfunktionen lassen sich die geschilderten datenschutzrechtlichen Probleme vermeiden, wenn anstelle von kontogebundenen Karten sog. White Cards verwendet werden, die nicht durch Abbuchung von einem Konto, sondern durch Bareinzahlung aufgeladen werden und damit keine Identifizierung des Inhabers ermöglichen. Sie sind als Alternative zur kontogebundenen GeldKarte bei den Kreditinstituten erhältlich.