Bezirksregierung Arnsberg

Bezirksregierung Arnsberg • Postfach • 59817 Arnsberg
An den
Präsidenten des Landtags NRW
Postfach 10 11 43

40002 Düsseldorf

Dienstgebäude:
Seibertzstr. 1
Auskunft erteilt
Ahlers
Telefon
02931/82-2371
Telefax
02931/82-2450
Mein Zeichen **(bitte stets angeben)**
21.8
Datum
31.01.2000

Betr.: Datenschutz
hier: Gesetz zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW)

Berichterstatter: Regierungsrat Sommer

Anlagen: 2

Zum Gesetz zur Änderung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) kann aus Sicht der Bezirksregierung Arnsberg als nachgeordneter Behörde, die für die Datenschutzaufsicht im nicht-öffentlichen Bereich zuständig ist, unter Einschränkung der Erfahrungen aus der Praxis Stellung genommen werden.

Vor dem Hintergrund der Diskussion um die Verlagerung der Datenschutzaufsicht im nicht-öffentlichen Bereich möchte ich eine Erfahrungsbericht der datenschutzrechtlichen Aufsichtstätigkeit sowie eine kurze Stellungnahme zum Diskussionspunkt „Zuständigkeitsverlagerung" abgeben.

1. Tätigkeitsbeschreibung

In den Jahren 1998 und 1999 sind gegen private datenverarbeitende Stellen bei der Bezirksregierung Arnsberg **361 Beschwerden** eingegangen. Diese richteten sich insbesondere gegen Auskunfteien, die Schufa, den Adresshandel, Versicherungen, Ärzte und Krankenhäuser. Bei der Prüfung dieser Eingaben sind im Regelfall zunächst schriftlich Stellungnahmen der datenverarbeitenden Firmen, gegen die sich die Beschwerde richtete, eingeholt worden. Darüber hinaus sind im Einzelfall auch Prüfungen vor Ort durchgeführt worden.

Ein auffallend großer Teil der Beschwerden betraf die Zulässigkeit und die Dauer der Speicherung von Negativdaten bei den Handelsauskunfteien und der Schufa. Ferner wurden sehr häufig die unerwünschte Zusendung von Werbeschreiben und die Herkunft des Adressmaterials von den Betroffenen beklagt.

Soweit Beanstandungen durch die Bezirksregierung Arnsberg ausgesprochen worden sind, sind diese von den datenverarbeitenden Stellen ausnahmslos beseitigt worden.

Weiterhin sind in den Jahren 1998 und 1999 über **300 allgemeine Anfragen und Beratungsersuchen** von betrieblichen Datenschutzbeauftragten, Betriebsräten, Geschäftsleitungen, Einzelpersonen, Vereinen und Verbänden an die Bezirksregierung Arnsberg gerichtet worden. Diese betrafen überwiegend Probleme der Bestellung eines betrieblichen Datenschutzbeauftragten und die Zulässigkeit der Erhebung und Verarbeitung personenbezogener Daten.

Im westfälischen Landesteil haben **588 Firmen ihre meldepflichtige Datenverarbeitung bei der Bezirksregierung Arnsberg angezeigt**. Im Rahmen der regelmäßigen Kontrolle bei diesen meldepflichtigen Stellen (Auskunfteien, Rechenzentren und Markt-

und Meinungsforschungsinstituten) sind in den letzten beiden Jahren **90 Überprüfungen** vor Ort durchgeführt worden.

Die Schwerpunkte bei solchen Prüfungen sind in der Anlage 1 und 2 dargestellt. Das Ergebnis einer Datenschutzprüfung wird den Firmen vor Ort mündlich und anschließend schriftlich mitgeteilt.

Zudem obliegt der Bezirksregierung Arnsberg in Westfalen die Aufsicht über Medien- und Teledienstеanbieter nach dem Mediendienste-Staatsvertrag sowie dem Informations- und Kommunikationsdienstegesetz. Über 60 Provider sind bereits aufgefordert worden, ihr Sicherheitskonzept darzulegen. Die Auswertung der vorgelegten Unterlagen dauert zurzeit noch an.

Schließlich werden im Bereich des Datenschutzes die Bußgeldverfahren nach dem Bundesdatenschutzgesetz und dem Landesdatenschutzgesetz durchgeführt (ca. 10 Verfahren p.a.).

Ein Tätigkeitsbericht der Aufsichtsbehörden wird regelmäßig erstellt.

2. Personalausstattung

Die Aufgaben für den Datenschutz im nicht-öffentlichen Bereich werden bei der Bezirksregierung Arnsberg wahrgenommen von einem Juristen (0,3 Stellenanteile), einem technischen Prüfer (1,0 Stellenanteile), einem Verwaltungssachbearbeiter (1,0 Stellenanteile) und einer Mischarbeitsplatz-Mitarbeiterin (0,3 Stellenanteile).

Aufgrund des steigenden Arbeitsanfalls im Bereich der Aufsicht über Medien- und Teledienstеanbieter wird eine Personalverstärkung für unumgänglich gehalten.

3. Einzelprobleme, Beispielsfälle aus der Kontrolltätigkeit

a) "Schwarze Listen"/Negativdateien von Unternehmen und Verbänden

Die Bezirksregierung Arnsberg hatte erfahren, dass eine Interessengemeinschaft für Subunternehmen im Transportgewerbe eine Liste der "Schwarzen Schafe" des Transportgewerbes erstellt hatte. Alle Sub- und Kleinunternehmen, die negative Erfahrungen (z.B. verschleppte, schlechte oder keine Zahlung, dubiose Gegenforderungen, schlechte Auslastung, Knebelverträge oder Ausschließlichkeitsverträge, allgemeiner Umgang, usw.) gemacht haben, sollten dies der Interessengemeinschaft mitteilen.

In einer Liste sind 80 Firmen aufgeführt worden, die der Interessengemeinschaft aufgrund dieser Informationen Anlass zu Bedenken gaben. Auf die Angabe der vorliegenden Gründe (negative Erfahrungen der Subunternehmen) ist verzichtet worden.

Seitens der Aufsichtsbehörde bestanden gegen die Verwendung dieser Liste erhebliche datenschutzrechtliche Bedenken. Insbesondere das Verfahren zur Datenerhebung wurde für datenschutzrechtlich unzulässig angesehen. Jedermann konnte telefonische Angaben über eine andere Person verbreiten, ohne dass diese Angaben objektiv nachgeprüft wurden oder nachprüfbar waren (z.B. durch Vollstreckungstitel oder Vertragskopien). Somit konnte jedenfalls nicht ausgeschlossen werden, dass schutzwürdige Belange des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung offensichtlich überwogen.

Die Interessengemeinschaft sagte zu, diese oder eine ähnliche Liste nicht mehr herauszugeben.

Ein vergleichbares Verfahren zeichnete sich im Hotel- und Gaststättengewerbe ab.

Mehrere Stellen wandten sich an die Bezirksregierung, weil sie beabsichtigten, eine Negativdatei über Hotelgäste zu führen. Aus einer solchen Datei sollten auf konkrete Anfrage eines Hotelbetriebes die gespeicherten Daten zu einer angefragten Person übermittelt werden. Durch diese Informationsweitergabe sollten Verluste für die Hotelbetreiber wegen zunehmender Kriminalität und sinkender Zahlungsmoral in der Hotelbranche reduziert werden.

Die datenschutzrechliche Prüfung ergab, dass gegen Dateien der geplanten Art keine grundsätzlichen Bedenken bestehen, sofern die Speicherung und Übermittlung sich in den rechtlichen Grenzen des § 29 BDSG halten und die Vorschriften über die Benachrichtigung des Betroffenen, die Auskunft an den Betroffenen und die Berichtigung, Löschung und Sperrung von Daten beachtet werden. Ferner ist den Betreibern der Datei mitgeteilt worden, dass die Speicherung und Weitergabe von Angaben über noch nicht rechtshängige Forderungen datenschutzrechtlich nicht zulässig sei. Auch ist darauf hingewiesen worden, dass die beabsichtigte Speicherung der Seriennummern amtlicher Ausweise durch das Gesetz über Personalausweise und das Passgesetz eingeschränkt werde.

Darüber hinaus wurde den datenverarbeitenden Stellen mitgeteilt, dass bezüglich der geplanten Hinweisdatei die Vorschriften über die Meldepflicht (§ 32 BDSG) zu beachten sind.

b) Scoring-Verfahren der Schufa

Vermehrt haben sich Betroffene gegen das von der Schufa eingeführte Bürcscoring-Verfahren gewandt.

Die Score-Informationen der Schufa sind das Ergebnis einer zahlenmäßigen Bewertung aller im Schufa-Datenbestand gespeicherten Informationen unter Anwendung statistisch-mathemati-

scher Verfahren. Hierdurch soll eine Wahrscheinlichkeit zur Beurteilung von Risiken prognostiziert werden. Interessierte Schufa-Vertragspartner können, ergänzend zu einer Auskunft über die zu einer Person bislang gespeicherten Daten, Scoring-Informationen erhalten. Hierbei handelt es sich um den **Score-Wert**, die dazugehörige **Quote**, den **Bereich** und die **Risikoklasse**.

Der **Score-Wert** besteht aus einem Datenfeld aus bis zu 6 numerischen Zeichen. Ausgegeben werden Score-Werte zwischen 1 (schlechtester Wert) und 1.000 (bester Wert). Die **Quote** stellt das Risiko einer Abwicklungsstörung bei Kreditverträgen mit einer Personengruppe gleichartigen Datenprofils dar. Das Datenfeld kann bis zu 5 alphanumerische Zeichen aufnehmen. Ausgegeben wird ein Prozentwert mit zwei Nachkommastellen. Das Datenfeld **"Bereich"** kann 6 alphanumerische Zeichen aufnehmen. Die Kennzeichnung des Bereiches korrespondiert mit der Höhe des Score-Wertes (niedrigster, riskantester Wertebereich = A; höchster, bester Wertebereich = I). Die **Risikoklasse** kann aus bis zu 33 alphanumerischen Zeichen bestehen. Der Text steht in Abhängigkeit von der Aussage im Feld "Bereich". Standardgemäß erhalten diese Felder die Hinweise "Risikoklasse A - I".

Die Score-Informationen werden ergänzend und zur schnelleren Interpretation des Gehalts einer Auskunft antragsbezogenen berechnet und den Schufa-Vertragspartnern mit einer vollständigen Auskunft zur Verfügung gestellt. Die betroffenen Bürger beanstandeten, dass die Schufa-Selbstauskunft keine Score-Informationen enthalte. Sie waren der Auffassung, dass auch solche Informationen vom Betroffenen abrufbar sein müssten.

Die Schufa verneint eine Auskunftspflicht an den Betroffenen im Hinblick auf § 34 Abs. 4 i.V.m. § 33 Abs. 2 Nr. 2 BDSG, da die Score-Informationen nur deshalb gespeichert würden, weil sie ausschließlich der Datensicherheit und Datenschutzkontrol-

le dienen. Sie würden nicht im Schufa-Datenbestand sondern in Log-Files gespeichert und könnten daher nicht Bestandteil einer Selbstauskunft sein.

Aus Sicht der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich ist dieses Ergebnis nicht zufriedenstellend, da die Schufa-Vertragspartner jederzeit Score-Informationen erhalten können, während der Betroffene weder die Score-Informationen noch die Bewertungskriterien, die für die Bildung der Score-Informationen maßgeblich waren, sowie deren Gewichtung erfahren kann. Wegen der grundsätzlichen und bundesweiten Bedeutung können die regional zuständigen Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich jedoch keine endgültige datenschutzrechtliche Beurteilung vornehmen. Daher erörtern bereits die obersten Aufsichtsbehörden der Länder mit den Vertretern der Schufa die Angelegenheit. Die Beratungsgespräche mit der Schufa dauern noch an.

C) Videoüberwachung

Ein weiteres und zunehmendes Aufgabengebiet im nicht-öffentlichen Bereich ist die Videoüberwachung. Nach der derzeitigen Rechtslage fällt die Videoüberwachung zwar nur unter die Vorschriften des Bundesdatenschutzgesetzes, soweit die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten in einer Datei im Sinne des Bundesdatenschutzgesetzes, d.h. digital, durchgeführt wird, jedoch ist dieses aufgrund des schnellen technischen Fortschreitens in diesem Sektor immer häufiger der Fall. Digitale Videoüberwachung findet beispielsweise schon jetzt Einsatz bei Spielbanken und Tankstellen, aber auch bei privaten Haushalten, die sich mit Hilfe derartiger Technik vor Vandalismus und Einbrechern schützen wollen.

Aus diesem Grund konnte im Laufe des letzten Jahres eine stetige Zunahme der Anfragen bezüglich der Zulässigkeit des Ein-

satzes von Videoüberwachungsanlagen genauso wie die Anzahl der Beschwerden über den Einsatz von Videoüberwachungsanlagen beobachtet werden.

Nach der Novellierung des Bundesdatenschutzgesetzes fällt voraussichtlich jede Videoüberwachung - unabhängig von der eingesetzten Technik - unter dieses Gesetz.

Insgesamt hat sich die Videoüberwachung zu einer festen Größe bei der Beschwerdebearbeitung als auch bei der Prüfung vor Ort entwickelt.

4. Verlagerung der Zuständigkeiten in der Datenschutzaufsicht

Die vorangegangenen Ausführungen belegen, dass die Bezirksregierungen Arnsberg und Köln über mehr als zwanzig Jahre Erfahrung und Wissen in der Datenschutzaufsicht verfügen. Beide Aufsichtsbehörden sind in dieser Zeit ständige und anerkannte Partner für die Bürgerinnen und Bürger sowie nicht-öffentlichen Stellen geworden. Hinsichtlich der weiteren Argumente für eine Aufsichtstätigkeit im nicht-öffentlichen Bereich durch die Bezirksregierungen verweise ich auf das dem Ausschuss vorliegende Schreiben der Regierungspräsidenten von Arnsberg und Köln an den Innenminister des Landes Nordrhein-Westfalen vom 12.01.2000.

Im Auftrag

(Sommer)

DIE BEZIRKSREGIERUNG ARNSBERG

Bericht über die aufsichtsbehördliche Prüfung
gemäß § 38 Bundesdatenschutzgesetz (BDSG)
vom

Gemeldete Stelle:

Prüfungsteilnehmer:

Prüfungsdauer:

Ort:

Inhalt:

1. Allgemeines:

Allgemeiner Geschäftszweck:

Gesamtzahl der Mitarbeiter:

Aushilfskräfte:

Mitarbeiter in der EDV:

Operatoren:

Programmierer:

Systemprogrammierer:

Arbeitsvorbereitung:

Arbeitsnachbereitung:

Datenerfassung:

EDV-Leiter:

Arbeitszeiten (Schichtbetrieb):

2. Auftragsdatenverarbeitung:

Die Prüfungsteilnehmer führten zunächst ein allgemeines Gespräch. Dabei wurde die Tätigkeit der zu prüfenden Stelle erörtert und festgestellt, dass automatisierte Datenverarbeitung für rechtlich Dritte betrieben wird. Es wurde darauf hingewiesen, dass die Auftragsdatenverarbeitung in jeder der in § 3 BDSG genannten Phasen (Speicherung, Löschung, Veränderung,

Übermittlung) nur im Rahmen der Weisungen des Auftraggebers gestattet ist (§ 11 BDSG).

Der Prüfer wurde über den Zweck der Datenverarbeitung, d.h. über die Art der Daten und ihre weitere Verwendung unterrichtet. Dies war zur Beurteilung der gemäß § 9 BDSG zu realisierenden Sicherungsmaßnahmen notwendig.

Datenverarbeitung wird für Auftraggeber im Bereich folgender Anwendungen betrieben:

Die Prüfungsteilnehmer stellten fest, dass die oben beschriebenen Tätigkeiten den besonderen Anforderungen § 11 BDSG unterliegen. Somit hat der Regierungspräsident Arnsberg - also die nach Landesrecht zuständige Aufsichtsbehörde für den Datenschutz - die Ausführung des Bundesdatenschutzgesetzes zu überwachen. Die Aufsicht erstreckt sich auf die Auftragsdatenverarbeitung nach § 11 BDSG.

3. Formalrechtlicher Bereich:

Im Bereich der formalrechtlichen Erfordernisse der zu prüfenden Stelle wurden folgende Punkte angesprochen:

3.1 Verpflichtung auf das Datengeheimnis nach § 5 BDSG

Der Gesetzgeber schreibt vor, dass es den bei der Datenverarbeitung beschäftigten Personen untersagt ist, geschätzte personenbezogene Daten unbefugt zu nutzen. Nach Absatz 2 dieser Vorschrift sind diese Personen bei Aufnahme ihrer Tätigkeit

auf das Datengeheimnis zu verpflichten. Zur Beachtung dieser Vorschrift wurde festgestellt:

3.2 Bestellung des betrieblichen Datenschutzbeauftragten (§ 36 BDSG)

Es wurde deutlich gemacht, dass die Frage der Bestellung des betrieblichen Datenschutzbeauftragten ungeachtet der Eigen- oder Fremddatenverarbeitung zu beurteilen ist. Maßgeblich ist nur die Anzahl der mit der Verarbeitung personenbezogener Daten beschäftigten Mitarbeiter der zu prüfenden Stelle. Nach § 36 Absatz 1 BDSG ist spätestens binnen eines Monats nach Aufnahme der Tätigkeit ein Beauftragter für den Datenschutz schriftlich zu bestellen, wenn mindestens fünf Mitarbeiter ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise (manuell) verarbeitet werden und hierbei in der Regel mindestens 20 Mitarbeiter ständig beschäftigt sind.

Für die zu prüfende Stelle wurde festgestellt, dass mindestens ... Personen mit der automatisierten Verarbeitung personenbezogener Daten betraut sind. Somit ist nach den Vorschriften des Bundesdatenschutzgesetzes ein betrieblicher Datenschutzbeauftragter erforderlich. Die schriftliche Bestellung des Herrn vom wurde vorgelegt.

Nach § 36 Absatz 2 BDSG darf zum betrieblichen Datenschutzbeauftragten nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Technische, organisatorische und rechtliche Kenntnisse sind bei der Fachkunde zu beachten:

Technische Kenntnisse:

Organisatorische Kenntnisse:

Rechtliche Kenntnisse:

Für die geforderte Zuverlässigkeit kann festgehalten werden, dass aufgrund der sonstigen wahrzunehmenden Aufgaben des Datenschutzbeauftragten ein erhebliches Konfliktpotential nicht vorhanden ist.

Es wurde darauf hingewiesen, dass der betriebliche Datenschutzbeauftragte der Geschäftsführung unmittelbar zu unterstellen ist. In Anwendung der Fachkunde auf dem Gebiet des Datenschutzes muss er weisungsfrei arbeiten können.

3.3 Aufgaben des betrieblichen Datenschutzbeauftragten:

Der betriebliche Datenschutzbeauftragte hat die Ausführung des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Zur Beurteilung der Pflichterfüllung hinsichtlich der im Bundesdatenschutzgesetz aufgestellten Anforderungen an den betrieblichen Datenschutzbeauftragten wurden folgende Punkte erörtert:

a) Übersicht über die Art der gespeicherten personenbezogenen Daten.

   Dies ist notwendig, um die in § 9 BDSG geforderten technischen und organisatorischen Maßnahmen sinnvoll treffen zu können. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck besteht. Eine Übersicht über die Art der gespeicherten personenbezogenen Daten konnte...

b) Datenverarbeitungsprogramme

Die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden, ist vom betrieblichen Datenschutzbeauftragten zu überwachen. Es wurde festgestellt, dass

c) Schulung der Mitarbeiter

Die bei der Verarbeitung personenbezogener Daten tätigen Personen sind mit den im Bundesdatenschutzgesetz festgelegten Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse im Geschäftsbereich des Unternehmens, vertraut zu machen. Der betriebliche Datenschutzbeauftragte nimmt diese Aufgaben in der Weise wahr, dass er

d) Auswahl der Mitarbeiter

Der Datenschutzbeauftragte soll bei der Auswahl der mit der Verarbeitung personenbezogener Daten beschäftigten Personen beratend mitwirken. Durch folgende Aktivitäten wird diese Aufgabe wahrgenommen:

3.4 Auftragsdatenverarbeitung (§ 11 BDSG)

Wie bereits eingangs festgehalten wurde, erörterten die Prüfungsteilnehmer die Vorschrift des § 11 BDSG. Der Gesetzgeber hat die Schriftform zum Nachweis vertraglicher Vereinbarungen nicht ausdrücklich vorgesehen. Für das geprüfte Unternehmen wurde festgestellt, dass

Es wurde darauf hingewiesen, dass für den Fall, dass die gemeldete Stelle Subunternehmer zur Durchführung von Datenverarbeitungsaufgaben eingesetzt, sie die Auftragnehmer unter besonderer Berücksichtigung der dort getroffenen technischen und organisatorischen Maßnahmen im Sinne des § 9 BDSG sorgfältig auszuwählen hat. Hierauf wies der Prüfer hin und verdeutlichte, dass Registermeldungen der Subunternehmer nicht als Nachweis für eine ordnungsgemäße Erledigung der übertragenen Aufgaben gewertet werden können und eine solche Meldung die Realisierung erforderlicher Sicherheitsmaßnahmen nicht bestätigt.

3.5 Meldepflicht und Registermeldung (§ 32 BDSG)

Aufgrund der Tätigkeit des Unternehmens besteht Meldepflicht nach § 32 BDSG. Danach war die Aufnahme der Tätigkeit beim RP Arnsberg binnen eines Monats anzumelden. Die dabei gemachten Angaben werden gemäß § 38 BDSG in einem öffentlichen Register geführt.

Änderungen zum Register sowie die Beendigung der Auftragsdatenverarbeitung sind der Aufsichtsbehörde stets mit Monatsfrist unaufgefordert anzuzeigen. Dies wurde gegenüber der geprüften Stelle deutlich gemacht.

Die Prüfungsteilnehmer kontrollierten die derzeitige Registermeldung und kamen zu folgendem Ergebnis:

4. Feststellungen zur Hard- und Software:

Die geprüfte Stelle setzt im Bereich der Auftragsdatenverarbeitung Hard- und Software folgender Art ein:

Computersystem:

DFÜ-Einrichtung:

Betriebssystem:

Sicherheitssystem:

Programmiersprachen:

Anwendungssoftware:

5. Technische und organisatorische Maßnahmen:

Ein wesentlicher Teil der Prüfung erstreckte sich auf die in § 9 BDSG geforderten technischen und organisatorischen Maßnahmen, die erforderlich sind, um die Ausführungen der Vorschriften des Bundesdatenschutzgesetzes, insbesondere die in der Anlage zum BDSG gemachten Anforderungen zu gewährleisten. Erforderlich sind die dort geforderten Sicherungsmaßnahmen dann, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck besteht.

1. Zugangskontrolle

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.

1.1 Räume mit DV-Anlagen:

- Welche Räume
- Unterschiedliche Sicherheitsstufen

1.2 Absicherung dieser Räume:

- Regelung der Zugangsberechtigung für Mitarbeiter, Pflege- und Wartungspersonal, Besucher.
- Anwesenheitsliste mit Name und Zeit
- Anwesenheit funktionsfremder Mitarbeiter
- Türsicherung (elektrische Türöffner, Magnetkarte, Chipkarte, Monitorüberwachung, Schlüssel, Ersatzschlüssel, Generalschlüssel)
- Ein- und Ausgänge im Rechenzentrum
- Optische und akustische Anzeige, wenn eine gesicherte Tür offensteht.

1.3 Flure und Gänge (Bewegungsmelder, Kameraüberwachung, Rauchmelder)

1.4 Außenhautsicherung

- Fenster (Glasbruchmelder, Anzeige, wenn nicht verschlossen)
- Geländeüberwachung (bewegungsempfindliche Kameras)
- Gesicherter Eingang bei Anlieferung oder Ablieferung

1.5 Kontrollraum, in dem Störungen gemeldet werden

- Ständig besetzt
- Besondere Sicherheitsvorkehrungen für diesen Raum.

1.6 Schwachstellen bei Nachtschicht

2. Abgangskontrolle:

Personen, die bei der Verarbeitung personenbezogener Daten tätig sind, sind daran zu hindern, dass sie Datenträger unbefugt entfernen.

1.7 Bereiche und Räume, in denen sich Datenträger befinden bzw. befinden dürfen.

1.8 Befugte Personen:

- Festlegen der Personen, die aus diesen Räumen Datenträger entfernen dürfen
- Ausweise der Abholberechtigten (Auftragspapiere, Begleitpapiere)

1.9 Aufbewahrung der Datenträger

- Datenträgerarchiv
- Buchführung der Datenträger und ihre Ausgabe
- Kopien, alte Versionen
- Zeitraum für Bestandskontrollen
- Vieraugenprinzip

1.10 Verbot der Mitnahme von Taschen und Koffern in die Maschinenräume bzw. Arbeitsräume.

1.11 Vernichtung der Datenträger

- EDV-Listen
- Eingabebelege
- Kohlepapier
- zerstörte Platten und Bänder.

2. Speicherkontrolle:

Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten ist zu verhindern.

2.1 Differenzierung der Befugnisse bei der Verarbeitung personenbezogener Daten.

- Wer darf eingeben, lesen, verändern, löschen.

2.2 User-ID/Passwort

- Vergabeverfahren (Systempasswort)
- Passwortlänge
- Passworte für Programme/Dateien
- Terminalkennung
- Zeitliche Begrenzung
- Änderung softwaremäßig erzwingen (vier Wochen)
- Änderung der Passwörter nach Urlaubsvertretung
- Neue Passwörter abgleichen mit bereits vorhandenen
- Mitschreiben von Fehlversuchen

2.3 Protokollierung der Datei- und Programmbenutzung (Konsolenprotokolle, Blattschreiber)

2.4 Verschlüsselungsroutinen

- Für User-ID/Passwörter (DES, Pbulic key, Einwegverschlüsselung)
- Für besonders sensible Daten
- Prüfziffern

2.5 Getrennte DV-Anlagen für Produktion und Entwicklung

3. Benutzerkontrolle:

Die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, ist durch Unbefugte zu verhindern.

3.1 Festlegen der Nutzungsberechtigten

3.2 Absicherung des DV-Systems

- Identifizierung des Benutzers (Chipkarte, Magnetkarte, Benutzerkennung)
- Zuordnung einzelner Terminals ausschließlich für bestimmte Anwendungen
- zeitliche Beschränkung von Terminals
- Systemprotokolle (Benutzerkennung; Gerätenummer, Zeit, Programm, Datum, Empfänger, ...)
- Protokollierung von Mißbrauchsversuchen
- Abschließen des Terminals
- Panel-Keys
- Chiffrierung

4. Zugriffskontrolle:

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die Ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können.

4.1 Dokumentation der Zugriffsberechtigung

4.2 Kontrolle des Zugriffs

- Identifikation des Zugreifenden bekannt
- Passworte für Programme und Dateien
- Zugriffsschutz bis auf Feldebene (zeitlich und inhaltlich abhängig)
- Protokollierung:

4.3 Wer darf Zugriffsbeschränkungen ändern

4.4 Maßnahmen bei wiederholten Fehlversuchen.

5. Übermittlungskontrolle:

Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können.

Es wird nicht verlangt zu protokollieren, an wen Daten übermittelt worden sind, sondern an wen Daten übermittelt werden können (Anlegen und Fortschreiben einer Übersicht, die erkennen läßt, an welche Stellen zu welcher Zeit welche personenbezogenen Daten selbsttätig an welche Empfänger übermittelt werden können).

5.1 Mögliche Empfänger (Dritte, an die übermittelt werden kann (namentlich benennen))

5.2 Wer darf senden

5.3 Welche Daten werden gesendet

5.4 Zeitpunkt und Ort der Übermittlung

6. Eingabekontrolle

Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem im Datenverarbeitungssystem eingegeben worden sind.

6.1 Festlegen, wer etwas eingeben darf

6.2 Kontrolle der Eingaben

- Protokolldatei (Platte/Drucker mit: Dateninhalt, Benutzerkennung und Zeit)
- Protokollierung der Operator-Aktivitäten (Konsolprotokoll)
- Dokumentation der gelaufenen Programme

6.3 Aufbewahrungszeitraum für obige Protokolle

7. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (§ 37 BDSG).

7.1 Form der Auftragserteilung

- Grundsätzlich schriftlich
- Beschreibung des Auftrags (welche Verarbeitung)
- Regelung für Verpackung und Versand der Datenträger
- Regelung nicht mehr benötigter Unterlagen (evtl. Vernichtung von Listen, Eingabebelegen)
- eindeutiger Auftraggeber (Festlegen der weisungsberechtigten Personen)

7.2 Prüfung der Identität des Auftraggebers bzw. seines Vertreters bei Rückgabe der Datenträger

7.3 Quittung bei Übergabe der Datenträger

7.4 Löschung von Restdaten (evtl. anderer Kunden)

7.5 Kontrolle der auftragsgemäßen Verarbeitung beim Auftragnehmer

- Zuständigkeit und Verantwortung
- Kontrollinstanzen (Vier-Augen-Prinzip)

8. Transportkontrolle

Es ist zu gewährleisten, dass bei der Übermittlung personenbezogener Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können.

8.1 Transport

- innerhalb der Unternehmung
- zwischen Auftraggeber und Auftragnehmer
- örtliche und zeitliche Festlegung der Übergabe
- Datenträgeraustausch (mit Banken)

8.2 Personen

- Auswahl der befugten Personen (Kurier, Bundesbahn, Post, Direktabholung)
- Ausweis des Transportpersonals (Ausweise, Auftragspapiere, Begleitpapiere, Quittungen)

8.3 Transportmittel

- Behälter
- abschließbar/versiegelt

9.4 Löschung

- vor dem Beschreiben mit neuen Daten
- nach dem Lesen der Daten (auftragsgemäß)

8.4 Transportsicherung bei Datenauslagerung

9. Organisationskontrolle

Die innerbehördliche oder innerbetriebliche Organisation ist so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

9.1 Lageplan, Organigramm, Datenflussplan, Verarbeitungsablauf

9.2 Festlegen der Aufgaben/Verantwortung eines Mitarbeiters (Stellenbeschreibung)

9.3 Funktionstrennung/räumliche Trennung

- AV, DT, MS, PRG, SYSPRG, SY STEC, AN

9.4 Richtlinien für die Programmierung

- Auftrag, Genehmigung, Durchführung, Kontrolle, Überwachung, Freigabe, Dokumentation
- Systemanalyse, Vorgehensmodell
- Programmänderung (Test, Vernichtung der Testergebnisse, Dokumentation)
- Übernahme von Produktionsprogrammen

9.5 Buchführung der Datenträger

- Verzeichnis der Dateien, Bänder, Platten, Disketten
- Verzeichnis über Lagerorte der Dateien, Bänder, Platten, Disketten

- Aufzeichnung der Datenträger, die z.Zt. nicht im Archiv sind

9.6 Kontrolle (Vier-Augen-Prinzip)

- Wer kontrolliert (DSB, weitere Instanzen)
- angemeldete/unangemeldete Kontrollen
- permanentes Fortschreiben der Kontrollmaßnahmen (Aufbauorganisation, Ablauforganisation)
- Auswertung der Protokolle des Maschinenraumes
- Aufbewahrung von Anwesenheitslisten und Systemprotokollen (wo und wie lange)

9.7 Katastrophenplan, Wiederinbetriebnahme

9.8 Dokumentation

- im Einsatz befindlicher Programme
- im Einsatz befindlicher Dateien
- Art der Daten

Bezirksregierung Arnsberg

Checkliste

zur Überprüfung der Auskunfteien nach § 32 Abs. 1 Satz 1 Nr. 1 BDSG

Firma:

Ort:

Datum:

Beginn:

Ende:

Teilnehmer Firma:

Teilnehmer Bezirksregierung:

1. Eröffnungsgespräch

1. Rechtsform der meldepflichtigen Stelle

natürliche Person

Inhaber

juristische Person des privaten Rechts

eingetragener Verein - e.V. - (§§ 55 ff BGB)

Vertretungsberecht. Vorst.-Mitgl.:

BGB-Gesellschaft (§§ 705 ff BGB)

Geschäftsf. Gesellschafter:

Offene Handelsgesellschaft - OHG - (§§ 105 ff HGB)

Geschäftsf. Gesellschafter:

Kommanditgesellschaft - KG - (§§ 161 ff HGB)

Pers. haft. Gesellschafter/Geschäftsführer:

Gesellsch. m. beschr. Haftung - GmbH - (§§ 1 ff GmbH)

Geschäftsführer:

Aktiengesellschaft - AG - (§§ 1 ff Akt. G)

Verantwortl. Vorst.-Mitgl.:

Genossenschaft (§§ 1 ff GenG)

Verantwortl. Vorst.-Mitgl.:

nichtrechtsfähiger Verein (§ 54 i.V.m. § 705 BGB)

Geschäftsf. Gesellschafter:

Eintragung im

Gewerberegister bei:

Vereinsregister

Handelsregister am:

Genossenschaftsregister

nicht eingetragen

Unternehmensgegenstand lt. Registereintragung:

2. Angaben zum Register

   Änderungen

   wann eingetragen:

   zu Punkt:

3. Organisation

   - interner Aufbau
   - Geschäftsverteilung/Zuständigkeiten
   - Raumplan

4. Anweisungen Datenschutz/Datensicherung

   - wann erstellt
   - für welche Bereiche (differenziert)

5. Vorrangige Rechtsvorschriften

   - Überwachung durch Aufsichtsbehörden, ggf. welche

6. Verpflichtung nach § 5 BDSG

   - Auswahl des Personenkreises (Kriterien)
   - Form
   - Aufklärung
   - Verfahren bei Neueinstellung/Versetzung

II. Beauftragter für den Datenschutz

I. Anzahl der im Unternehmen beschäftigten Arbeitnehmer (vgl. § 6 Betr.VG)

insgesamt=

davon entfallen auf

Vollzeitkräfte =
Halbtagskräfte =
Aushilfen =
Auszubildende =
Heimarbeiter =

Mit der Verarbeitung personenbezogener Daten sind in

automatisierten Verfahren =

nicht automatisierten Verfahren =

beschäftigt.

2. Bestellung des betr. DSB

2.1: Zeitpunkt und Form

2.2: Hauptfunktion

2.3: Fachkunde

- Lehrgänge, Seminare
- Erfa-Kreis

2.4: Unmittelbare Unterstellung

- Organisationsplan

3. Aufgaben des betr.: DSB

3.1: Unterstützung durch weitere Stellen

- Datenschutzarbeitskreis
- Datensicherheitsbeauftragte

3.2: Schulung, Aufklärung

- in welcher Form
- in welchen Zeitabständen
- wann zuletzt
- Verfahren bei Neueinstellung

3.3: Mitwirkung bei der Personalauswahl

- Form

3.4: Dateienübersicht nach § 38 i.V.m. § 29 BDSG

- Bezeichnung der Dateien, in denen personenbezogene Daten gespeichert werden
- Angaben über die Art der gespeicherten Daten
- Geschäftszwecke oder Ziele, zu deren Erfüllung gerade diese Daten notwendig sind
- diejenigen Dritte, denen regelmäßig, das ist ständig wiederkehrend, solche Daten übermittelt werden
- Art der eingesetzten Datenverarbeitungsanlagen nach
  - Hersteller
  - Typ
  - Einrichtungen der Datenfernverarbeitung und deren Standort

---

- Schreibautomat (Textverarbeitungssystem)
  Steuerung über Systemprogramm
  Zentraleinheit
  Speichermedium (z.B. Disketten, Kassetten, Magnetplatten oder Magnetstreifenkarten)

III. Datenerhebung/-Speicherung:

1. Nachbarschaftsbefragung

a) befragter Personenkreis

Vermieter

Nachbar

Ehegatte

Arbeitgeber

andere

b) abgefragte Daten beschränkt auf

Wohnort/Aufenthaltsdauer

Einkommen

Arbeitgeber

wirtschaftliche Verhältnisse/evtl.

Bankverbindung

andere Daten, ggf. welche:

c) Anzahl der Befragungen (Bagatellfälle)

d) Angaben durch Recherchebogen überprüfbar

2. Selbstbefragung

a) Angaben überprüfbar

3. Registerauswertung

Handelsregister

Vereinsregister

Genossenschaftsregister

Schuldnerregister

Melderegister

4. Inkassoauswertung

Welche Daten im Einzelfall

5. Schätzdaten

a) begrenzt auf folgende Fälle

Alter (nur Geburtsjahr)
Einkommen
Betriebszahlen
Grundstückswert

b) Schätzgrundlage

Inaugenscheinnahme (Recherchebogen)
Einkommenstabelle/Bewertungsliste etc.
andere, ggf. welche:

6. Krediturteil = internes Datum, wenn

nach Übermittlung der Auskunft gespeicherte zur nochmaligen Weitergabe nicht geeignet = Kreditfrage überprüfen!
nicht-automatisierte abgespeichert

III. Datenübermittlung:

1) berechtigtes Interesse glaubhaft dargelegt

a) Anfrageschein Bürgel

b) Anfrageschein Creditreform

Eigene Erfahrungen mit der Zahlungsweise des Kunden:

- ☐ Skontozahler
- ☐ vereinbarungsgemäß
- ☐ langsam
- ☐ Protest, gerichtliche Maßnahmen

Sonstiges:

Bitte FREIUMSCHLAG mit Ihrer genauen Anschrift zur Vermeidung von Verzögerungen und Irrtümern beifügen.

Es wird versichert, daß der Anfrage eine Kreditentscheidung zugrunde liegt, sofern nicht ein anderer Anfragegrund angekreuzt ist (§ 32 Abs. 2 BDSG)

1 Bonitätsprüfung	5 Versicherungsvertrag
2 Geschäftsanbahnung	6 Beteiligung
3 Forderung	7 .....

c) Anfrageschein Schimmelpfeng

Bitte unbedingt beachten! Gemäß § 32 Abs. 2 BDSG wird versichert, daß diese Auskunft für eine Kreditentscheidung benötigt wird, sofern nicht einer der nachstehend aufgeführten Gründe angekreuzt bzw. benannt ist.

- ☐ Bonitätsbeurteilung für eine beabsichtigte Geschäftsverbindung
- ☐ Bonitätsbeurteilung für eine bestehende Geschäftsverbindung
- ☐ Forderungseinzug
- ☐ Warenkreditversicherung
- ☐ Versicherungsvertrag
- ☐ Leasingvertrag
- ☐ Mietvertrag

Sonstiger Grund

Zahlweise bisher	Vereinbarte Zahlweise in Tagen	durchschnittlich bezahlt nach Tagen	Kreditlinie DM
	Anmerkungen (z. B. Negativmerkmale)		

2. Stichprobe zur Überprüfung des berechtigten Interesses

Anzahl der Stichproben
nach welchen Kriterien
Feststellungen/Auswertungen

3. Nachträge bei Betroffenen zulässig, wenn

3.1 beschränkt auf
eidesstattliche Versicherung
Haftanordnung
erhebliche Wechselproteste, wenn
eine gewisse Häufung eintritt
Häufung von Einziehungsverfahren
bei sonst unbestrittenen Forderungen

3.2 und sie innerhalb einer Frist von 6 Monaten nach Auskunftserteilung abgegeben werden.

4. Übermittlung an Arbeitgeber

4.1 Personaleinstellung wird ausdrücklich angegeben

4.2 der wirtschaftliche Bezug ist eindeutig

5. Schutzwürdige Belange nicht beeinträchtigt

Persönliche Beurteilung
Aufgrund der hier angeführten/aufgeführten
Tatsachen wird der Betroffene positiv
beurteilt/beurteilen wir den Betroffenen
Nachbarschaftsbefragung
Schätzdaten
Registerauswertung
Inkssoauswertung

V. Datenveränderung:

= das inhaltliche umgestalten gespeicherter Daten

Welche gespeicherten Daten werden übermittelt?
Werden dadurch schutzwürdige Belange beeinträchtigt:

VI. Auskunft an den Betroffenen

1. Benachrichtigung

Zeitpunkt
Form
dokumentiert

bei Ergänzungsberichten
Archivmitteilungen
Vorberichten

2. Auskunft

2.1 schriftlich

2.2 Inhalt der Auskunft

aktuelle Daten
Hinweis auf gesperrte Daten
Persönliche Beurteilung
ggf. Krediturteil

2.3 Entgelt

bei Auskunft über gesperrte Daten

- Kalkulation -

zurückgezahlt bei
unrichtiger
Speicherung
unzulässiger

2.4 Beschwerden von Betroffenen überprüfen

VII. Berichtigung:

1. durch die speichernde Stelle

- z.B. aus unmittelbar zugänglichen öffentlichen Quellen
- Änderungsdienst

2. auf Antrag des Betroffenen

VIII. Sperrung:

1. Richtigkeit wird vom Betroffenen bestritten

2. am Ende des 5. Kalenderjahres nach der Einspeicherung

Überprüfung des Fristablaufs (Sperrvermerk)
interne Auswertung
Übermittlung vorgenommen
- Gründe -

12/3689

IX. Löschung:

1. Zulässigkeit gegeben bei Nichtbeeinträchtigung schutzwürdiger Belange

2. bei unzulässiger Speicherung

3. Betroffener verlangt Löschung nach 5. Kalenderjahr

4. Richtigkeit kann nicht bewiesen werden bei

   - gesundheitlichen Verhältnissen
   - strafbaren Handlungen
   - Ordnungswidrigkeiten
   - religiöse Anschauungen
   - politische

5. Auszüge aus dem Schuldnerverzeichnis

X. Allg. Datensicherung