ADV-Gesamtplan für die Hochschulen des Landes Nordrhein-Westfalen

Sachverständigen-Arbeitsgruppe für die Erstellung eines Gesamtplanes für die Automatisierte Datenverarbeitung an den Hochschulen des Landes Nordrhein-Westfalen

Düsseldorf, 1980

A.5 Vorläufige Richtlinien zur Durchführung des Bundesdatenschutzgesetzes vom 21. Februar 1979

urn:nbn:de:hbz:466:1-12345

F 4763 A

MINISTERIALBLATT

FÜR DAS LAND NORDRHEIN-WESTFALEN

32. Jahrgang	Ausgegeben zu Düsseldorf am 22. März 1979	Nummer 17

Inhalt

I.

Veröffentlichungen, die in die Sammlung des bereinigten Ministerialblattes für das Land Nordrhein-Westfalen (SMBl. NW.) aufgenommen werden.

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

I.

Vorläufige Richtlinien zur Durchführung des Bundesdatenschutzgesetzes

RdErl. d. Innenministers v. 21. 2. 1979 – I A 3/52 – 09.00

Inhaltsübersicht

Die Landesregierung hat durch die Verordnung über Zuständigkeiten nach dem Bundesdatenschutzgesetz vom 10. Januar 1978 (GV. NW. S. 16/SGV. NW. 20061) den Regierungspräsidenten Arnsberg für die Regierungsbezirke Arnsberg, Detmold und Münster und den Regierungspräsidenten Köln für die Regierungsbezirke Düsseldorf und Köln zu Aufsichtsbehörden gem. §§ 30/40 Bundesdatenschutzgesetz (BDSG) vom 27. Januar 1977 (BGBl. I S. 201) bestimmt.

Die örtliche Zuständigkeit der Aufsichtsbehörden richtet sich nach § 3 Abs. 1 Nr. 2 VwVfG NW.

Die Regierungspräsidenten haben bei der Durchführung der Aufsicht zunächst folgende Richtlinien zu beachten:

1 Allgemeine Regelungen

1.1 Anwendungsbereich des BDSG

Das BDSG bestimmt als Aufgabe des Datenschutzes, der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken; jedoch unterliegen nur „personenbezogene Daten", die in „Dateien" verarbeitet werden, dem Gesetz (§ 1 Abs. 1 u. 2 Satz 1 BDSG).

Das BDSG ist ein Auffanggesetz; Rechtsvorschriften des Bundes, die auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, gehen dem BDSG vor. (Vgl. § 45 Nr. 1–8 BDSG; die Aufzählung ist nicht erschöpfend.)

Das BDSG gilt grundsätzlich für die Datenverarbeitung öffentlicher und privater Stellen.

Nordrhein-Westfalen nutzt den Vorbehalt zu Gunsten der Landesverwaltung in § 7 Abs. 2 BDSG aus. Für die Datenverarbeitung öffentlicher Stellen des Landes Nordrhein-Westfalen und der seiner Aufsicht unterstehenden juristischen Personen des öffentlichen Rechts gilt daher nicht das BDSG, sondern das Datenschutzgesetz Nordrhein-Westfalen (DSG NW) vom 19. Dezember 1978 (GV. NW. S. 640/SGV. NW. 20061). Auf die Gerichte und Behörden der Staatsanwaltschaft findet das DSG NW jedoch nur Anwendung, soweit sie Verwaltungsaufgaben wahrnehmen; im übrigen gilt für sie das BDSG.

1.2 Allgemeine Ausnahmen und Einschränkungen

1.21 Medienprivileg

Dem BDSG unterliegen nicht personenbezogene Daten, die durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden (§ 1 Abs. 3 BDSG).

Unabhängig davon unterliegen alle in Dateien verarbeiteten personenbezogenen Daten den Datensicherungsvorschriften des § 6 Abs. 1 und, sofern sie in automatisierten Verfahren verarbeitet werden, der Anlage zum BDSG.

1.22 Interne Dateien

Für Dateien, die lediglich internen Zwecken dienen, deren Daten also nicht zur Übermittlung an Dritte bestimmt sind und in nicht automatisierten Verfahren betrieben werden, gelten die Vorschriften des Gesetzes ebenfalls nicht; gemäß § 1 Abs. 2 Satz 2 BDSG sind lediglich die Datensicherungsvorschriften des § 6 anzuwenden. Daten, die zwar noch nicht übermittelt wurden, die aber ihrer Art nach aufgrund gesetzlicher Vorschriften oder nach ihrer sonstigen Zweckbestimmung zur Übermittlung bestimmt sind, unterliegen voll dem BDSG.

Eine gelegentliche Übermittlung von Daten entgegen der sonst aufrechterhaltenen Zweckbestimmung schließt deren internen Charakter nicht aus. Die Übermittlung selbst unterliegt jedoch den Vorschriften des BDSG.

1.3 Abgrenzung zwischen drittem und viertem Abschnitt

Für die Datenverarbeitung privater Stellen bringt das BDSG unterschiedliche Regelungen je nach dem, ob die Datenverarbeitung für eigene oder für fremde Zwecke geschieht. Das BDSG regelt den Datenschutz für die Datenverarbeitung aller privater Stellen.

Die gleiche juristische oder natürliche Person kann mit bestimmten Anwendungen der Datenverarbeitung den Vorschriften des dritten Abschnittes unterliegen, für bestimmte andere Bereiche denen des vierten Abschnittes. Im einzelnen:

1.31 Anwendung des dritten Abschnitts

Wer personenbezogene Daten in Dateien für eigene Geschäftszwecke oder Ziele verarbeitet, hat die Vorschriften des dritten Abschnittes des BDSG einzuhalten. Dabei kommt es nicht darauf an, ab die tatsächliche Datenverarbeitung durch den Normadressaten selbst oder in seinem Auftrag durch andere (z. B. Service-Rechenzentren) durchgeführt wird. Entscheidend ist, für wessen Zwecke oder Ziele die Daten verarbeitet werden, in wessen Verfügungsgewalt sie sind; wer also „Herr" der Daten ist.

1.32 Anwendung des vierten Abschnitts

1.321 Anwendungsfälle

Die Vorschriften über die geschäftsmäßige Datenverarbeitung privater Stellen für fremde Zwecke (vierter Abschnitt) gliedern sich in drei Hauptanwendungsbereiche:

- Datenverarbeitung zum Zwecke der Übermittlung an andere (§ 31 Abs. 1 Nr. 1 BDSG); Hauptanwendungsfälle: Auskunfteien, Adreßhändler, Adressverlage
- Verarbeitung zu anonymisierender Daten (§ 31 Abs. 1 Nr. 2 BDSG); Hauptanwendungsfälle: Markt- und Meinungsforschungsinstitute
- Datenverarbeitung als Dienstleistungsunternehmen für andere (§ 31 Abs. 1 Nr. 3 BDSG); Hauptanwendungsfälle: Service-Rechenzentren, Datenerfassungsbüros.

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

In allen Fällen ist Voraussetzung, daß die Datenverarbeitung geschäftsmäßig geschieht, also auf Wiederholung gerichtet ist; Gewinnerzielungsabsicht ist nicht notwendig.

1.322 Datenverarbeitung im Auftrag

In der Praxis wird häufig die Datenverarbeitung „außer Haus" durchgeführt. Verpflichtet nach den Vorschriften des dritten Abschnitts oder nach §§ 32 bis 36 BDSG bleibt dann der Betrieb, für den die Daten verarbeitet werden.

Welcher Art die Rechtsbeziehungen zwischen Auftraggeber und Auftragnehmer sind, ist dabei unbeachtlich. Besondere Gestaltung kann dieses Rechtsverhältnis finden, wenn in verbundenen Unternehmen (Konzernen) eine Gesellschaft die Datenverarbeitung auch für die anderen Gesellschaften betreibt (vgl. dazu Nr. 1.33 und Nr. 1.35).

Wer geschäftsmäßig als Dienstleistungsunternehmen die Datenverarbeitung im Auftrag übernimmt, hat die einschlägigen Vorschriften des vierten Abschnitts einzuhalten (§ 31 Abs. 1 Nr. 3 BDSG). Er darf insbesondere nur nach den Weisungen des Auftraggebers die Daten verarbeiten (§ 37 BDSG). Er muß ferner die notwendigen Maßnahmen zur Datensicherung (§ 6 BDSG) und zur Wahrung des Datengeheimnisses (§ 5 BDSG) treffen.

1.33 Verpflichtete Unternehmen

Das BDSG geht von einer juristischen, nicht von einer wirtschaftlichen Betrachtungsweise aus.

Verpflichtet ist die einzelne natürliche oder juristische Person. Außer Betracht bleiben dabei Beteiligungsverhältnisse an einer anderen juristischen Person, z. B. bei verbundenen Unternehmen (Konzernen). Die Pflichten aus dem Gesetz treffen jeweils die einzelne Gesellschaft.

1.34 Grenzfälle

Wird Datenverarbeitung teils für eigene, teils für fremde Zwecke betrieben, dann ist im Grundsatz für den Fremdanteil der vierte Abschnitt anzuwenden.

Ein geringfügiger Anteil der Fremdarbeiten kann jedoch ein Anzeichen dafür sein, daß die Datenverarbeitung insoweit nicht geschäftsmäßig als Dienstleistungsunternehmen betrieben wird. Dabei sind verschiedene Fälle denkbar:

1.341 Zeigt die Organisation der Datenverarbeitung oder des Rechenzentrums eine Ausprägung als Dienstleistungsunternehmen, findet für den als Auftragsdatenverarbeitung abgrenzbaren Teil immer der vierte Abschnitt Anwendung.

1.342 Haben einzelne Rechenzentren eines Unternehmens ausschließlich die Aufgabe der Auftragsdatenverarbeitung (Kundenrechenzentren), so findet auf diese Rechenzentren der vierte Abschnitt Anwendung.

1.343 Ist in den sonstigen Fällen der Anteil der Auftragsdatenverarbeitung im Verhältnis zur Gesamtdatenverarbeitung des Unternehmens geringfügig, dann spricht das dafür, daß die Datenverarbeitung nicht geschäftsmäßig als Dienstleistungsunternehmen betrieben wird. Es ist dann nur der dritte Abschnitt anzuwenden.

1.35 Sonderfall:

Verbundene Unternehmen/Konzerne betreiben häufig die Datenverarbeitung für mehrere oder alle der einzelnen Gesellschaften gemeinschaftlich. Betreibt eine Gesellschaft die Datenverarbeitung für den Konzern und gleichzeitig auch für die eigene juristische Person, dann ist für den „Eigenanteil" der dritte Abschnitt anzuwenden. Für den Teil der Datenverarbeitung, der für andere Konzernunternehmen durchgeführt wird, gilt im Grundsatz der vierte Abschnitt.

Zu unterscheiden sind jedoch zwei Fälle:

1.351 Wird eine gesamte Aufgabe (z. B. Vertrieb) einschließlich der Datenverarbeitung auf eine Gesellschaft im Konzern als Funktion übertragen, findet nur der dritte Abschnitt Anwendung. Geschäftszweck im Sinne des § 22 Abs. 1 BDSG ist im genannten Beispiel auch der Vertrieb.

1.352 Verbleibt die Verwaltung, die personenbezogene Daten verarbeitet, als Funktion bei den einzelnen Gesellschaften und wird lediglich die tatsächliche Datenverarbeitung von einer anderen Konzerngesellschaft betrieben, dann werden von letzterer die Daten im Auftrag der anderen Gesellschaften verarbeitet. Geschieht das geschäftsmäßig als Dienstleistungsunternehmen, dann findet wegen § 31 Abs. 1 Nr. 3 BDSG der vierte Abschnitt Anwendung.

1.4 **Geltung des BDSG bei grenzüberschreitendem Datenverkehr**

1.41 Das BDSG ist auch anzuwenden, wenn personenbezogene Daten von im Ausland lebenden Betroffenen im Inland verarbeitet werden.

1.42 Wird die Verarbeitung personenbezogener Daten von rechtlich selbständigen ausländischen Tochtergesellschaften eines deutschen Unternehmens im Inland vorgenommen, dann sind zwei Fälle zu unterscheiden:

1.421 Der Muttergesellschaft im Inland sind Teile der Verwaltung auch für die ausländische Tochtergesellschaft als eigene Funktion übertragen. Dann fällt die Datenverarbeitung unter den dritten Abschnitt des BDSG.

1.422 Die Verwaltung bleibt ungeschmälert Aufgabe der ausländischen Tochter. Die Muttergesellschaft betreibt dann insoweit Auftragsdatenverarbeitung, es findet der vierte Abschnitt Anwendung.

1.43 Personenbezogene Daten dürfen an ausländische Tochtergesellschaften unter den gleichen Voraussetzungen wie an Dritte im Inland übermittelt werden. Schutzwürdige Belange des Betroffenen werden nicht schon dadurch beeinträchtigt, weil es im Empfängerland kein Datenschutzgesetz gibt.

1.5 **Begriffsbestimmungen**

Das BDSG definiert wichtige Begriffe in § 2 und an anderen Stellen; es weicht dabei mitunter vom üblichen Sprachgebrauch ab. Um eine gleichmäßige Anwendung des Gesetzes zu erreichen, ist bis auf weiteres von folgendem auszugehen:

1.51 Personenbezogene Daten

Personenbezogene Daten im Sinn des Gesetzes sind „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)" (§ 2 Abs. 1 BDSG).

Dabei sind Einzelangaben Daten, die den Betroffenen bestimmen oder bestimmbar machen.

Einzelangaben sind aber auch Daten, die einen in der Person des Betroffenen liegenden oder auf den Betroffenen bezogenen Sachverhalt beschreiben; auch Werturteile, Planungs- und Prognosedaten über den Betroffenen gehören dazu.

Die Einzelangaben können persönliche oder sachliche Verhältnisse einer Person betreffen.

Die Daten müssen einer natürlichen Person zugeordnet werden können.

Nicht geschützt sind Daten über juristische Personen oder über Personenvereinigungen.

Die natürliche Person muß bestimmt (z. B. durch Identifizierungsdaten) oder bestimmbar sein (z. B. durch Bezugnahme auf andere Daten oder äußere Umstände). Aggregierte Daten sind nicht personenbezogen; enthält die statistische Gruppe nur Angaben über eine oder zwei Personen, dann sind die Daten wieder personenbezogen.

Bei personenbezogenen Daten, bei denen die speichernde Stelle Namen und Anschrift des Betroffenen nicht kennt, ist sie von der Einhaltung solcher Bestimmungen entbunden, die eine solche Kenntnis voraussetzen.

1.52 Datei

Datei ist eine „gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkma-

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

len umgeordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren" (§ 2 Abs. 3 Nr. 3 BDSG).

Es kommt nicht darauf an, ob die Daten in konventionellen Verfahren oder in automatisierten Verfahren (vgl. dazu Nr. 1.92) verarbeitet werden. In aller Regel werden die in Datenverarbeitungsanlagen verarbeiteten Datensammlungen den Dateibegriff erfüllen. Abgrenzungsschwierigkeiten kann es bei manuell geführten Dateien geben. Dazu wird auf folgendes hingewiesen:

Gleichartig aufgebaut ist eine Sammlung von Daten, die sich entweder auf einem einzigen oder auf mehreren physisch gleichartigen Datenträgern befindet.

Die gespeicherten Daten müssen auf dem Datenträger in einer bestimmten Ordnung enthalten sein, also in einer für die Datenverarbeitung geeigneten Weise formalisiert und formalisiert auf dem Datenträger untergebracht sein. Die Sammlung selbst muß noch nicht geordnet sein, sie muß aber nach bestimmten Merkmalen geordnet werden können.

Merkmale sind nicht alle Daten, sondern nur solche, nach denen die Sammlung geordnet und ausgewertet werden kann. „Freie Texte" sind in der Regel keine Merkmale.

Die Zahl der in der Datei enthaltenen Betroffenen ist unerheblich.

Datei im Sinne des Gesetzes sind jedenfalls – neben den in Computern verarbeiteten – Karteien, Sichtlochkarteien, Randlochkarteien, Sammlungen von Lochkarten, Sammlungen von Schecks, Tickets und dergleichen.

Datei sind nicht Akten oder Aktensammlungen. Zwar bezieht § 2 Abs. 3 Nr. 3 BDSG sie wieder in den Dateibegriff ein, wenn sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können. Derzeit sind jedoch Verfahren nicht bekannt, die beide Anforderungen erfüllen.

1.53 Speichern

Speichern ist das „Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung" (§ 2 Abs. 1 Nr. 1 BDSG).

Das Erfassen von Daten unterliegt dem BDSG nur, wenn der Datenträger eine Datei enthält oder selbst Dateibestandteil ist (z. B. Karteikarte). Noch nicht erfaßt im Sinne des Gesetzes sind somit Daten auf Urbelegen oder Erfassungsbelegen, die nur zum Aufbau einer Datei benutzt werden; sie werden erst mit Übertragung auf den Datenträger der Datei „erfaßt".

Das Speichern im Sinne des Gesetzes endet mit dem Löschen der Daten (dazu Nr. 1.55) oder wenn die Daten nicht mehr zum Zwecke ihrer weiteren Verwendung aufbewahrt werden, z. B. wenn ein Magnetband zum Überschreiben mit anderen Daten freigegeben wird.

1.54 Sperren

Gesperrte Daten sind „mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden" (vgl. §§ 14 Abs. 2 Satz 3, 27 Abs. 2 Satz 3, 35 Abs. 2 Satz 3 BDSG).

Auf diese Weise gesperrt werden können

- einzelne Daten eines Betroffenen, z. B. in einem Feld einer Karteikarte oder eines Datensatzes
  - Einzelsperre,
- alle Daten eines Betroffenen, auch in mehreren Dateien
  - Datensatzsperre – und
- der Inhalt ganzer Sammlungen, z. B. eine gesamte Datei oder Teile davon
  - Sammelsperre.

Demzufolge kann der „Sperrvermerk" in verschiedener Weise bewirkt werden. Bei der Einzelsperre muß sich aus dem Sperrvermerk ergeben, welche einzelnen Daten gesperrt sind. Bei der Datensatzsperre genügt es, wenn der Sperrvermerk auf der Karte vermerkt ist oder sich aus ihm ergibt, welcher Datensatz gesperrt ist (z. B. bei Anlage einer Sperrdatei).

Bei der Sammelsperre (z. B. Daten, die nach Zeitablauf archiviert werden) genügt es, wenn der Sperrvermerk allgemein angebracht wird (z. B. eine gesamte Kartei oder ausgesonderte Teile davon wird sichtbar mit dem Vermerk „Gesperrt" versehen; Magnetbänder oder Magnetplatten werden an einer besonderen Stelle des Archivs abgelegt und mit dem Vermerk „Gesperrt" versehen).

Gesperrte Daten bleiben gespeichert, sie unterliegen der Berichtigungspflicht und müssen unter bestimmten Voraussetzungen auch gelöscht werden. Die Berichtigung kann bei Archivbeständen (§§ 14 Abs. 2 Satz 2, 27 Abs. 2 Satz 2 und 35 Abs. 2 Satz 2 BDSG) solange unterbleiben, bis diese Datenbestände wieder genutzt werden (§ 14 Abs. 2 Satz 3 BDSG). Gesperrte Daten dürfen nicht mehr verarbeitet oder – z. B. für interne Auswertungen – sonst genutzt werden. Praktisch bedeutsam ist dabei vor allem, daß gesperrte Daten nicht mehr übermittelt werden dürfen. Erlaubt ist die Nutzung nur unter den Voraussetzungen des § 14 Abs. 2 Satz 3 BDSG. Ob einer dieser Fälle vorliegt, hat die speichernde Stelle in eigener Verantwortung zu entscheiden.

Sind die Daten nach Ablauf einer bestimmten Frist zu sperren (vgl. § 35 Abs. 2 Satz 2 BDSG), genügt es, wenn der Fristablauf vor einer beabsichtigten Verarbeitung oder sonstigen Nutzung überprüft wird.

1.55 Löschen

Löschen ist „das Unkenntlichmachen gespeicherter Daten" (§ 2 Abs. 2 Nr. 4 BDSG). Daten sind unkenntlich gemacht, wenn sie von Menschen nicht mehr zur Kenntnis genommen werden können. Das kann in verschiedener Form geschehen. Auf Papier können Schriftzeichen durch Ausstreichen, Überschreiben oder Schwärzen unkenntlich gemacht werden, aber auch durch Vernichten des Datenträgers Papier.

Können Daten nur unter Zuhilfenahme technischer Mittel durch den Menschen zur Kenntnis genommen werden, dann sind sie unkenntlich, wenn durch technische oder organisatorische Mittel sichergestellt ist, daß sie von niemandem zur Kenntnis genommen werden können. Das kann durch Neuformierung der Magnetschichten (z. B. Überschreiben) geschehen, wodurch die Daten für die Verarbeitungsanlage nicht mehr lesefähig sind.

Das Gesetz fordert nicht ein physisches Vernichten der Daten. Deshalb können z. B. einzelne Daten auf Sicherungsbändern auch dadurch gelöscht werden, daß durch geeignete organisatorische Maßnahmen sichergestellt ist, daß sie nicht mittels Datenverarbeitung „zur Kenntnis genommen" werden.

1.6 **Aufgaben der Aufsichtsbehörden**

Die Aufgaben der Aufsichtsbehörden sind in §§ 30, 39 und 40 BDSG abschließend normiert. Sie unterscheiden sich danach, ob die zu beaufsichtigende private Datenverarbeitung den Vorschriften des dritten oder des vierten Abschnittes des BDSG unterliegt. Im einzelnen:

1.61 Datenverarbeitung für eigene Zwecke

Wer personenbezogene Daten als Hilfsmittel zur Erfüllung eigener Geschäftszwecke oder Ziele verarbeitet, unterliegt insoweit nur einer sogenannten Anlaßaufsicht. Die Aufsichtsbehörden werden gemäß § 30 Abs. 1 BDSG nur tätig, wenn

1.611 entweder ein Betroffener ihnen gegenüber begründet darlegt, daß er bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden ist oder

1.612 wenn der Beauftragte für Datenschutz des Unternehmens sie um Unterstützung bittet.

1.62 Datenverarbeitung für fremde Zwecke

Soweit jemand personenbezogene Daten geschäftsmäßig für andere verarbeitet, sind die Aufgaben der Aufsichtsbehörde weiter gefaßt. Gemäß § 40 Abs. 1

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

BDSG werden die Aufsichtsbehörden außer in den Fällen der Nr. 1.611 und 1.612 auch tätig, indem sie

1.621 die Anmeldungen der Unternehmen nach § 39 BDSG entgegennehmen und darüber ein Register führen,

1.622 ständig die Ausführung der einschlägigen Datenschutzvorschriften überwachen (§ 40 Abs. 1 BDSG).

1.63 Anrufung durch einen Betroffenen (Nr. 1.611)

Wendet sich ein Betroffener an die Aufsichtsbehörde, ist in der Regel wie folgt zu verfahren:

Der Betroffene muß begründet darlegen, daß er in seinen Rechten verletzt worden ist. Soweit nicht schon in der Anrufung geschehen, bittet die Aufsichtsbehörde den Betroffenen um möglichst konkrete Darlegung des Sachverhalts. Allgemein gehaltene Behauptungen, die Ausforschungsuntersuchungen notwendig machen, weist sie mit dem Hinweis auf die Rechtslage zurück. Sie fordert den Betroffenen ggf. auf, einschlägige Unterlagen vorzulegen, aus denen sich ausreichende Hinweise für eine Rechtsverletzung ergeben.

Wurde die Rechtsverletzung vom Betroffenen schlüssig dargelegt und begründet, so hat er einen Rechtsanspruch auf Tätigwerden der Behörde. Im Regelfall fordert die Aufsichtsbehörde zunächst denjenigen, gegen den sich die Vorwürfe richten, zu einer schriftlichen Stellungnahme auf. Bringt diese keinen hinreichenden Aufschluß oder verbleibt der Verdacht, daß die Datenverarbeitung nicht ordnungsgemäß durchgeführt wird und deswegen der Betroffene in seinen Rechten weiterhin verletzt ist, dann kann die Aufsichtsbehörde Untersuchungen an Ort und Stelle veranlassen.

Ist nach dem ermittelten Sachverhalt anzunehmen, daß eine Rechtsverletzung zwar gegeben aber in Zukunft nicht mehr zu befürchten ist, dann verweist die Aufsichtsbehörde den Beschwerdeführer auf den Rechtsweg. Es ist nicht ihre Aufgabe, etwaige Rechte des Beschwerdeführers gegenüber dem Beanstandeten durchzusetzen. Soweit mit dem Auskunftsverweigerungsrecht nach § 26 Abs. 4 und § 34 Abs. 4 BDSG sowie mit der Geheimhaltungspflicht des § 30 VwVfG NW vereinbar, kann die Aufsichtsbehörde dabei dem Beschwerdeführer den ermittelten Sachverhalt mitteilen. Der Beanstandete ist entsprechend zu verständigen.

Soweit Rechtsverletzungen auch in Zukunft zu besorgen sind, legt die Aufsichtsbehörde dem Träger der Datenverarbeitung Maßnahmen nahe, die künftig eine Rechtsverletzung ausschließen. Sie soll dabei zu Einzelfragen den Datenschutzbeauftragten des Unternehmens heranziehen.

Stellt die Aufsichtsbehörde bei der Untersuchung eine Ordnungswidrigkeit fest, leitet sie ein Bußgeldverfahren ein. Liegt eine strafbare Handlung vor, verständigt sie die zuständige Staatsanwaltschaft.

1.64 Unterstützung des Datenschutzbeauftragten (Nr. 1.612)

Wendet sich der Datenschutzbeauftragte eines Unternehmens mit der Bitte um Unterstützung an die Aufsichtsbehörde, dann berät sie ihn im Rahmen ihrer Möglichkeiten zweckentsprechend.

1.65 Meldepflicht und regelmäßige Überwachung

Wer geschäftsmäßig personenbezogene Daten für fremde Zwecke verarbeitet (vierter Abschnitt BDSG), unterliegt der Meldepflicht nach § 39 BDSG und einer regelmäßigen Überwachung durch die Aufsichtsbehörde nach § 40 BDSG.

1.651 Meldepflicht (Nr. 1.621)

Die Aufsichtsbehörden nehmen die Anmeldungen nach § 39 BDSG entgegen; vgl. auch Nr. 1.8. Betrifft die Anmeldung eine Zweigniederlassung oder unselbständige Zweigstelle, dann übersenden die Aufsichtsbehörden einen Abdruck der Anmeldung der für den Sitz oder die Hauptverwaltung zuständigen Aufsichtsbehörde.

Die Aufsichtsbehörden führen über die Anmeldung ein Register. Das Register kann von jedermann eingesehen werden (§ 40 Abs. 1 Satz 2 BDSG).

1.652 Regelmäßige Überwachung (Nr. 1.622)

Aufgrund des Registers legen die Aufsichtsbehörden einen Überwachungsturnus fest.

Die Überwachungsberichte werden von der Aufsichtsbehörde ausgewertet.

1.7 **Befugnisse der Aufsichtsbehörden**

Den Aufsichtsbehörden werden durch § 30 Abs. 2 und 3 BDSG bestimmte Rechte eingeräumt. Diese sind

- Auskunftsverlangen,
- Betreten von Grundstücken und Geschäftsräumen zu Prüfungen und Besichtigungen sowie
- Einsichtnahme in geschäftliche Unterlagen.

Die Aufsichtsbehörden können diese Rechte selbst oder durch Beauftragte wahrnehmen. Zu Besichtigungen an Ort und Stelle ist der Beauftragte für den Datenschutz des Unternehmens hinzuzuziehen; ihre Ergebnisse sind mit ihm zu erörtern.

Das BDSG räumt den Aufsichtsbehörden jedoch keine besonderen Befugnisse ein, festgestellte Mängel durch behördliches Einschreiten abzustellen. Werden bei Betrieben, die der Gewerbeordnung unterliegen, schwerwiegende Mängel festgestellt, dann sind diese der zuständigen Behörde mitzuteilen. Werden Ordnungswidrigkeiten nach § 42 BDSG festgestellt, dann kann ggf. mit Geldbuße vorgegangen werden.

1.8 **Meldepflicht**

Wer geschäftsmäßig Datenverarbeitung für fremde Zwecke betreibt (vierter Abschnitt BDSG – vgl. Nr. 1.32–1.35), muß das der Aufsichtsbehörde binnen eines Monats nach der Aufnahme der Tätigkeit melden.

1.81 Verpflichtete Stelle

Meldepflichtig sind sowohl das Unternehmen als auch Zweigniederlassungen und unselbständige Zweigstellen. Das können sein:

- natürliche Personen,
- juristische Personen,
- Gesellschaften, z. B. BGB-Gesellschaft, offene Handelsgesellschaft, Kommanditgesellschaft,
- sonstige Personenvereinigungen des privaten Rechts, z. B. nicht rechtsfähige Vereine, Parteien, Gewerkschaften,
- Zweigniederlassungen der genannten Stellen, und zwar solche, die nach § 13 HGB, § 42 AktG, § 12 GmbHG und § 14 GenG zum Handelsregister anzumelden sind,
- unselbständige Zweigstellen der genannten Stellen, das sind organisatorische Einheiten, die nach außen mit einer gewissen Selbständigkeit auftreten.

Wer innerhalb des Unternehmens oder der sonstigen Stelle die Anmeldung vorzunehmen hat, bestimmt die interne Regelung des Unternehmens oder der sonstigen Stelle; der Anmeldende muß nur ausreichend legitimiert sein. Es kann auch die Zentrale die Anmeldung für alle Zweigniederlassungen und unselbständige Zweigstellen durchführen.

1.82 Inhalt der Meldepflicht

Die Anmeldung muß folgenden Inhalt haben (§ 39 Abs. 2 BDSG):

1. Name oder Firma der Stelle (die Bezeichnung, unter der die Stelle im Geschäftsverkehr auftritt); bei Zweigniederlassungen und unselbständigen Zweigstellen auch Name der Hauptstelle.
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder verfassungsmäßig berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen; bei Zweigniederlassungen und unselbständigen Zweigstellen auch Name der Hauptstelle;
   - die Personen, die für die Leitung des Unternehmens, der Zweigniederlassung oder der unselbständigen Zweigstelle verantwortlich sind;

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

- die Personen, die den Bereich Datenverarbeitung verantwortlich leiten;

3. Anschrift der meldepflichtigen Stelle; bei Zweigniederlassungen und unselbständigen Zweigstellen auch Name der Hauptstelle.
4. Geschäftszwecke oder Ziele der Stelle und der Datenverarbeitung;
   - Geschäftszwecke und Ziele des Unternehmens, ähnlich den Angaben, die zum Handelsregister oder Vereinsregister gemacht werden müssen;
   - Zwecke und Ziele der Verarbeitung personenbezogener Daten;
5. Art der eingesetzten automatisierten Datenverarbeitungsanlagen: Hersteller, Typ, Einrichtungen der Datenfernverarbeitung und deren Standort;
6. Name des Beauftragten für den Datenschutz;
7. Art der gespeicherten personenbezogenen Daten, das ist eine Kurzbeschreibung der Inhalte der gespeicherten Daten, z. B. Namen, Anschrift, Familienstand;
8. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten;
   - Name, Anschrift;
   - Art der übermittelten Daten entsprechend Nr. 7.

Wer Auftragsdatenverarbeitung im Sinne des § 31 Abs. 1 Nr. 3 BDSG betreibt, braucht in der Meldung die nach Nr. 7 und 8 geforderten Angaben nicht zu machen.

1.83 Zuständige Aufsichtsbehörde

Die Meldung ist an die zuständige Aufsichtsbehörde zu richten. Zuständig ist die Aufsichtsbehörde, in deren Bereich der Betrieb oder die Betriebsstätte gelegen ist, in welchem die Datenverarbeitung betrieben wird; vgl. dazu auch Nr. 1.81.

1.9 Der Datenschutzbeauftragte des Unternehmens

1.91 Verpflichtete Unternehmen

Natürliche oder juristische Personen, die Datenverarbeitung für eigene Zwecke oder geschäftsmäßig Datenverarbeitung für fremde Zwecke betreiben, haben von einem bestimmten Umfang der Datenverarbeitung an einen Beauftragten für den Datenschutz zu bestellen (§§ 28, 38 BDSG). Verpflichtet zur Bestellung ist unter den gesetzlichen Voraussetzungen jede einzelne natürliche oder juristische Person. Wirtschaftliche Zusammenhänge zwischen mehreren juristischen oder natürlichen Personen (Mehrheitsverhältnisse, verbundene Unternehmen) bleiben insoweit außer Betracht; vgl. jedoch Nr. 1.94.

1.92 Voraussetzungen für die Ernennung

Einen Datenschutzbeauftragten muß bestellen, wer personenbezogene Daten entweder

- in automatisierten Verfahren verarbeitet und hierbei in der Regel mindestens fünf Arbeitnehmer ständig beschäftigt oder
- in manuellen Verfahren verarbeitet und hierbei in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt.

Automatisierte Verfahren sind solche, in denen wesentliche Verfahrensschritte (z. B. Erfassung, Speicherung, Übermittlung, Veränderung) mit Hilfe programmgesteuerter Geräte ablaufen.

Zu berücksichtigen sind sämtliche Arbeitnehmer, die innerhalb des Unternehmens bei der Datenverarbeitung beschäftigt sind. Bei automatisierten Verfahren gehören dazu nicht nur die unmittelbar in Rechenzentren und im Bereich der Systementwicklung und Programmierung Beschäftigten, sondern auch Arbeitnehmer, die zentral oder dezentral Daten erfassen oder verändern (Off-line oder On-line).

Ständig beschäftigt ist ein Arbeitnehmer, der nicht nur vorübergehend in seiner Hauptbeschäftigung in der Datenverarbeitung tätig ist; gelegentlich anderweitige Tätigkeiten bleiben außer Betracht. In der Regel in der Datenverarbeitung beschäftigt sind auch solche Arbeitnehmer, die nur periodisch, aber in kürzeren Abständen, etwa in den letzten Wochen eines jeden Monats, dafür eingesetzt werden.

Verarbeitet ein Unternehmen personenbezogene Daten teils in automatisierten, teils in manuellen Verfahren, dann muß die Mindestzahl (fünf oder zwanzig) mindestens in einer der Verarbeitungsarten erreicht sein.

Vergibt ein Unternehmen die Datenverarbeitung „außer Haus", behält es aber die Datenerfassung, dann ist das in der Datenerfassung beschäftigte Personal zu berücksichtigen.

1.93 Persönliche Voraussetzungen

Der Datenschutzbeauftragte muß die erforderliche Fachkunde und Zuverlässigkeit haben. Fachkunde ist notwendig auf dem Gebiete der Datenverarbeitung, der betrieblichen Organisation und der einschlägigen Gesetze. Erfüllt der Datenschutzbeauftragte nicht von Anfang an alle Voraussetzungen, dann muß er jedenfalls die Fähigkeit haben, sich in die anderen Gebiete einzuarbeiten.

Der Datenschutzbeauftragte muß nicht ausschließlich mit den Funktionen des Datenschutzbeauftragten betraut sein. Besonders in kleineren Unternehmen kann er noch andere Tätigkeiten wahrnehmen, sofern das die Erfüllung seiner Aufgaben als Datenschutzbeauftragter nicht beeinträchtigt.

Inhaber, Vorstände, Geschäftsführer und sonstige gesetzlich oder verfassungsmäßig berufene Leiter können nicht zum Datenschutzbeauftragten ihres Unternehmens bestellt werden. Zum Datenschutzbeauftragten sollen darüber hinaus solche Personen nicht bestellt werden, die in dieser Funktion in Interessenkonflikte geraten würden, die über das unvermeidliche Maß hinausgehen; das liegt z. B. nahe, wenn der Leiter der EDV, der Personalleiter oder bei Direktvertrieb der Vertriebsleiter zum Datenschutzbeauftragten bestellt werden soll.

Der Datenschutzbeauftragte kann Arbeitnehmer des Unternehmens sein. Das Unternehmen kann aber auch einen „Externen" zum Datenschutzbeauftragten bestellen. Er ist vertraglich so zu verpflichten, daß er die Aufgaben eines Datenschutzbeauftragten entsprechend den Vorschriften des BDSG wahrnehmen kann. Ihm müssen auch die zur Erfüllung seiner Aufgaben nach §§ 28 und 29 BDSG notwendigen Rechte eingeräumt werden. Der „externe" Datenschutzbeauftragte kann die gleiche Aufgabe auch in anderen Unternehmen wahrnehmen. Dabei muß gewährleistet sein, daß er seine Aufgaben für jedes Unternehmen ordnungsgemäß erfüllen kann.

1.94 Datenschutzbeauftragte im Konzern

Es bestehen keine Bedenken, wenn verbundene Unternehmen die gleiche Person in den einzelnen rechtlich selbständigen Gesellschaften zum Datenschutzbeauftragten bestellen. Er muß von jeder Gesellschaft besonders bestellt und jeder Gesellschaft gesondert verantwortlich sein. Es muß dann sichergestellt sein, daß er für jede Gesellschaft seine Aufgaben ordnungsgemäß erfüllen kann.

1.95 Auftragsdatenverarbeitung

Service-Rechenzentren mit der entsprechenden Größe müssen selbst einen Datenschutzbeauftragten bestellen (§ 38 BDSG; vgl. Nr. 1.91). Wer seine Datenverarbeitung für eigene Zwecke (dritter Abschnitt) ganz oder teilweise „außer Haus" gibt, braucht nur dann selbst einen Datenschutzbeauftragten zu bestellen, wenn er selbst (in seinem Unternehmen) die nach Nr. 1.92 genannte Zahl der Beschäftigten erreicht.

1.96 Stellung und Aufgaben des Datenschutzbeauftragten

Der Datenschutzbeauftragte ist dem Vorstand oder dem sonst zur Leitung des Unternehmens Berufenen dafür verantwortlich, daß der Datenschutz im Unternehmen gewahrt wird (§ 28 Abs. 3 BDSG). Er muß der Unternehmensleitung aufgrund seiner Fachkunde die notwendigen Entscheidungsgrundla-

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

gen liefern. Dazu muß er u. a. (§ 29 BDSG) eine Übersicht mit folgendem Inhalt führen:

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

1.97 Zusammenarbeit mit der Aufsichtsbehörde

Der Datenschutzbeauftragte kann sich nach § 30 Abs. 1 Satz 2 BDSG in Zweifelsfällen an die Aufsichtsbehörde mit der Bitte um Unterstützung wenden. Die Aufsichtsbehörden beraten den Datenschutzbeauftragten im Rahmen ihrer Möglichkeiten.

Der Datenschutzbeauftragte ist nur von Unternehmen mit geschäftsmäßiger Datenverarbeitung für fremde Zwecke der Aufsichtsbehörde zu melden (§ 39 Abs. 2 Nr. 6 BDSG). In den anderen Fällen vergewissert sich die Aufsichtsbehörde über die Identität des Datenschutzbeauftragten in angemessener Form.

2 Datensicherung – Allgemeine Grundsätze –

2.1 Wesen der Datensicherung

Das BDSG verwendet zwar nicht den Begriff „Datensicherung", regelt aber die in § 6 und der Anlage zu § 6 Abs. 1 Satz 1 BDSG die Maßnahmen der Datensicherung, soweit sie für den Datenschutz von Bedeutung sind. Im einzelnen:

2.11 Begriff

Unter Datensicherung allgemein sind die technischen und organisatorischen Maßnahmen zu verstehen, die eine störungsfreie und gegen Mißbrauch gesicherte Datenverarbeitung zum Ziel haben. Solche Maßnahmen sind für jede Art von Datenverarbeitung unerläßlich; besonders wichtig sind sie in automatisierten Verfahren. Jede Störung oder Verzögerung der Datenverarbeitung kann schwerwiegende Folgen haben.

Soweit Maßnahmen zur Datensicherung auch dem Datenschutz im Sinne von § 1 Abs. 1 BDSG zu dienen geeignet sind, werden sie durch § 6 und die Anlage zu § 6 Abs. 1 Satz 1 BDSG gesetzlich vorgeschrieben. Durch geeignete technische und organisatorische Vorkehrungen soll die Erfüllung der Vorschriften des BDSG gewährleistet werden, also der Beeinträchtigung schutzwürdiger Belange des Betroffenen durch Mißbrauch bei der Datenverarbeitung entgegengewirkt werden. Dabei greift das Gesetz teilweise die für das Funktionieren der Datenverarbeitung ohnehin notwendigen Maßnahmen auf, teilweise geht es im Interesse eines wirksamen Datenschutzes darüber hinaus.

2.12 Anwendungsbereich

§ 6 BDSG gilt für jede Verarbeitung personenbezogener Daten in Dateien, in automatisierten ebenso wie in nichtautomatisierten Verfahren. Auch die nur internen Zwecken dienenden manuellen Dateien (§ 1 Abs. 2 Satz 2 BDSG) und die ausschließlich eigenen publizistischen Zwecken dienenden Dateien (§ 1 Abs. 3 BDSG) unterliegen den Vorschriften über die Datensicherung.

Das Gesetz stellt in § 6 Abs. 1 Satz 1 BDSG eine Grundregel der Datensicherung für jede Verarbeitung personenbezogener Daten in Dateien auf: Es sind immer alle erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Für automatisierte Verfahren wird das Gesetz konkreter: In der Anlage zu § 6 Abs. 1 Satz 1 BDSG definiert es bestimmte Anforderungen für zehn Bereiche; die zur Datensicherung verpflichtete Stelle hat sie mit entsprechenden Maßnahmen auszufüllen.

2.2 Verpflichtete Stelle

Zu Datensicherungsmaßnahmen nach § 6 Abs. 1 BDSG ist jeder verpflichtet, der im Rahmen des § 1 Abs. 2 BDSG oder im Auftrag der dort genannten Personen oder Stellen personenbezogene Daten verarbeitet. Verpflichtet ist somit einmal die speichernde Stelle im Sinne des § 2 Abs. 3 Nr. 1 BDSG, zum anderen aber auch jede Stelle, die im Auftrag speichernder Stellen Daten verarbeitet (§ 8 BDSG für öffentliche Stellen und § 31 Abs. 1 Nr. 3 BDSG i. V. mit § 37 BDSG für nicht-öffentliche Stellen).

Beauftragt eine speichernde Stelle ganz oder teilweise eine andere Stelle mit der Durchführung der Datenverarbeitung (vgl. Nr. 2.32), dann ist die Verantwortung für die Durchführung der Datensicherung auf den Auftraggeber und den Auftragnehmer verteilt:

2.21 Der Auftraggeber hat bei Erteilung des Auftrages die vom Auftragnehmer vorgesehenen Datensicherungsmaßnahmen zu berücksichtigen; die Wirksamkeit dieser Maßnahmen ist ein Auswahlkriterium für die Vergabe des Auftrages (§ 22 Abs. 2 Satz 2, § 31 Abs. 2 Satz 2 BDSG). Dem Auftraggeber müssen aber nicht notwendigerweise alle im einzelnen getroffenen Datensicherungsmaßnahmen offengelegt werden; dies könnte zu einer Ausspähung der Datensicherung für bestimmte Bereiche führen.

2.22 Der Auftraggeber hat ferner bei konkreten Anhaltspunkten den Auftragnehmer auf die Einhaltung der Datensicherungspflichten hinzuweisen. Zu Besichtigungen und Kontrollen an Ort und Stelle ist er nur insoweit befugt, als die vertraglichen Beziehungen ein solches Vorgehen erlauben.

2.23 Der Auftragnehmer ist für die Einhaltung der Datensicherung in allen Phasen der Datenverarbeitung, die er tatsächlich abwickelt, voll verantwortlich.

2.24 Soweit der Auftraggeber Teile der Datenverarbeitung tatsächlich selbst ausführt, trägt er insoweit die alleinige Verantwortung für die notwendige Datensicherung.

2.25 Fragen der zivilrechtlichen Haftung bleiben unberührt.

2.3 Notwendigkeit einzelner Maßnahmen

2.31 Rechtsgrundlagen

Nach § 6 Abs. 1 BDSG sind die zur Ausführung der Vorschriften des Gesetzes erforderlichen Maßnahmen der Datensicherung zu treffen; dies gilt sowohl für nichtautomatisierte als auch für automatisierte Verfahren. Für automatisierte Verfahren legt die Anlage zu § 6 Abs. 1 Satz 1 BDSG ergänzend Anforderungen für zehn einzelne Bereiche vor, die durch konkrete Maßnahmen auszufüllen sind; vgl. dazu Nr. 3. Das Gesetz schreibt solche Maßnahmen jedoch nicht konkret vor.

2.32 Verantwortung des Verpflichteten

Der zur Datensicherung Verpflichtete (vgl. Nr. 2.2) muß in eigener Verantwortung unter den in Betracht kommenden technischen und organisatorischen Maßnahmen der Datensicherung jene auswählen, die den vom Gesetz vorgeschriebenen Schutz der Daten gewährleisten. Sie sind vor dem Einsatz eines neuen oder geänderten Verfahrens im einzelnen festzulegen und mit Beginn des Einsatzes zu realisieren. Der Verpflichtete muß der Aufsichtsbehörde die Maßnahmen in geeigneter Form darlegen können.

Der Datenschutzbeauftragte ist zu beteiligen. Zu den Aufgaben des Datenschutzbeauftragten gehört es auch, die Wirksamkeit der Datensicherung zu überwachen. Stellt er Mängel fest, dann unterrichtet er unverzüglich den für den jeweiligen Bereich Verantwortlichen. In Zweifelsfällen kann er sich an die Aufsichtsbehörde wenden.

Im Falle der Auftragsdatenverarbeitung wirken Auftraggeber und Auftragnehmer zusammen. Ver-

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

antwortlich ist dabei jeweils derjenige, in dessen Tätigkeitsbereich die jeweiligen Maßnahmen der Datensicherung fallen. Für das gesamte Verfahren trägt der Auftraggeber im Rahmen der in Nr. 2.2 genannten Grundsätze die Verantwortung.

2.33 Summe der Maßnahmen

Für die Wirksamkeit der Datensicherung ist die Summe aller Maßnahmen entscheidend. Die Datensicherung ist dann ausreichend, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen hinreichenden Schutz gegen die Beeinträchtigung schutzwürdiger Belange des Betroffenen durch Mißbrauch seiner Daten gewährleisten.

Anforderungen, die für bestimmte Verfahren nicht relevant sind (z. B. Auftragskontrolle, wenn keine Auftragsdatenverarbeitung vorliegt), brauchen nicht berücksichtigt zu werden.

2.34 Angemessenheit der einzelnen Maßnahme

Eine Datensicherungsmaßnahme ist nicht schon allein deshalb zu treffen, weil sie objektiv geeignet ist, ein Höchstmaß an Datensicherung zu gewährleisten. Alle Maßnahmen zur Datensicherung stehen unter dem Grundsatz der Angemessenheit (§ 6 Abs. 1 Satz 2 BDSG). Eine Maßnahme braucht dann nicht getroffen zu werden, wenn der durch sie verursachte Aufwand im Verhältnis zu dem vom Gesetz verlangten Schutz der Daten unangemessen groß wäre. Dieser Grundsatz darf jedoch nicht dazu führen, die dem Gesetz unterliegende Datenverarbeitung ohne jede Sicherung zu lassen. Soweit im Einzelfall eine Anforderung nicht durch angemessene Maßnahmen voll erfüllt wird, ist die dadurch entstehende Lücke durch entsprechende Maßnahmen zur Erfüllung anderer Anforderungen zu schließen; vgl. auch Nr. 2.33 Absatz 1.

Ob eine Maßnahme als verhältnismäßig im Sinne des § 6 Abs. 1 Satz 2 BDSG anzusehen ist, kann nur anhand der konkreten Umstände des Einzelfalles entschieden werden. Dabei ist zwischen dem vom Gesetz verlangten Schutz der Daten und dem durch die Maßnahme verursachten Aufwand abzuwägen.

Als Entscheidungshilfen bei der Angemessenheitsprüfung können neben der Art der verarbeiteten Daten und ihrer Schutzwürdigkeit auch die Menge der verarbeiteten Daten sowie die Art der eingesetzten Verfahren dienen.

So erfordern z. B. Angaben über gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen weitergehende Datensicherungsmaßnahmen. Gleiches gilt, je mehr Daten über einen Betroffenen gespeichert werden. Die Verarbeitung von personenbezogenen Daten in einem großen Datenverarbeitungssystem (z. B. mit Hilfe einer Datenbank) kann wegen der vielfältigeren Nutzungsmöglichkeiten strengeren Anforderungen an die Datensicherung unterliegen.

3 Datensicherung
– Anforderungen und Maßnahmen für automatisierte Verfahren –

3.0 Anforderungen für automatisierte Verfahren; Erläuterung zentraler Begriffe

3.01 Anforderungen für automatisierte Verfahren

Die zur Datensicherung verpflichtete Stelle (vgl. Nr. 2.2) hat nach den in Nr. 2.33 und 2.34 dargelegten Grundsätzen die Anforderungen der Anlage zu § 6 Abs. 1 Satz 1 BDSG zu erfüllen (vgl. jedoch Nr. 2.33 Absatz 2 und 2.34 Absatz 1 Satz 4).

Der Anforderungskatalog der Anlage zu § 6 Abs. 1 Satz 1 BDSG ist nicht abschließend. Häufig wird es notwendig sein, auch nicht in der Anlage aufgeführte Bereiche durch Datensicherungsmaßnahmen abzudecken. Die Verpflichtung hierzu ergibt sich unmittelbar aus § 6 Abs. 1 Satz 1 BDSG. Dies gilt beispielsweise für den Bereich der Datenübertragung innerhalb der speichernden Stelle bzw. zwischen Auftraggeber und Auftragnehmer bei Auftragsdatenverarbeitung.

Die zehn Anforderungen der Anlage werden in diesem Abschnitt erläutert. An die Erläuterung ist jeweils angeschlossen eine Zusammenstellung in Betracht kommender Maßnahmen, mit denen die Anforderungen erfüllt werden können. Die dort aufgeführten Beispiele für Maßnahmen sind nicht abschließend; sie können auch nicht die für den Einzelfall erforderlichen Entscheidungen ersetzen.

3.02 Erläuterung zentraler Begriffe

3.021 Datenverarbeitungsanlage

Eine Datenverarbeitungsanlage ist die Gesamtheit der Baueinheiten, aus denen eine Funktionseinheit zur Verarbeitung von Daten aufgebaut ist (vgl. auch DIN 44 300).

Dazu gehören Zentraleinheiten und programmgesteuerte Geräte, einschließlich Geräte der angeschlossenen Peripherie (z. B. Leser, Drucker, Band- und Plattenlaufwerke, Stapelstationen sowie die über Stand- oder Wählleitungen angeschlossenen Terminals).

Nicht dazu zählen Geräte wie Kartenlocher, -prüfer, -doppler, Lochstreifen-Stanzer, die nicht an eine Zentraleinheit angeschlossen sind; für sie gilt § 6 Abs. 1 BDSG.

3.022 Datenverarbeitungssystem

Ein Datenverarbeitungssystem ist eine Funktionseinheit zur Verarbeitung von Daten (vgl. DIN 44 300), bestehend aus Datenverarbeitungsanlage(n) und Software.

3.023 Benutzung eines Datenverarbeitungssystems

Unter Benutzung eines Datenverarbeitungssystems ist jede Tätigkeit zu verstehen, mit der ein datenverarbeitender Vorgang in einem Datenverarbeitungssystem eingeleitet oder durchgeführt wird.

3.024 Selbsttätige Einrichtungen

Selbsttätige Einrichtungen werden verwendet, wenn Daten im On-line-Betrieb verarbeitet werden.

3.025 Unbefugt

Unbefugt handeln Personen dann, wenn ihre Tätigkeit nicht im Rahmen der ihnen übertragenen Aufgaben oder einer anderweitigen Ermächtigung liegt.

3.026 Datenträger

Ein Datenträger ist ein Mittel, auf dem Daten aufgezeichnet werden können. Datensicherungsmaßnahmen sind jedoch nur für Datenträger zu treffen, auf denen personenbezogene Daten aufgezeichnet sind (vgl. § 1 Abs. 1, Abs. 2 BDSG).

Das sind bei automatisierter Datenverarbeitung sowohl die verarbeitbaren (z. B. Magnetbänder, -platten, Lochkarten, Lochstreifen und optisch lesbare Belege) als auch die dabei erstellten Datenträger (z.B. Ausdrucke, Mikrofilmausgaben einschließlich ihrer Kopien).

3.1 Zugangskontrolle

3.11 Text der Anlage zum BDSG

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

3.12 Erläuterungen

3.121 Datenverarbeitungsanlage:

Siehe Nr. 3.021

3.122 Unbefugte:

Siehe Nr. 3.025, bezogen auf den Zugang zu Datenverarbeitungsanlagen.

3.123 Zugang:

Zugang ist die Annäherung an Datenverarbeitungsanlagen in der Weise, daß hierdurch eine Möglichkeit entsteht, auf diese einzuwirken oder von Daten Kenntnis zu nehmen.

3.124 Verarbeitung von Daten:

Hierunter sind die in § 2 Abs. 2 Nr. 1 bis 4 BDSG definierten Verarbeitungsphasen Speichern, Übermit-

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

teln, Verändern und Löschen zu verstehen, soweit sie mit Hilfe von Datenverarbeitungsanlagen erfolgen.

3.13 Zielrichtung

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, daß Unbefugte Zugang zu solchen Datenverarbeitungsanlagen haben, mit denen mindestens eine der vier Phasen der Verarbeitung personenbezogener Daten durchgeführt wird. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.14 Verfahrensschritte

- Festlegung von Sicherungsbereichen
- Absicherung der Zugangswege
- Festlegung von Zugangsberechtigungen einschließlich ihrer Dokumentation
  - für Mitarbeiter der Behörden/Firmen
  - für Behörden-/Firmenfremde (Wartungspersonal, Besucher usw.)
- Legitimation der Zugangsberechtigten
- Kontrolle des Zugangs

3.15 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)

- Festlegung befugter Personen
- Berechtigungsausweise
- Regelungen für Behörden-/Firmenfremde
- Anwesenheitsaufzeichnungen
- Besucherausweise
- Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage und/oder Werkschutz
- Sicherheitsbereiche und wenig Zugangswege schaffen
- Schlüsselregelung
- Gesicherter Eingang für An- und Ablieferung
- Türsicherung (elektrischer Türöffner, Ausweisleser, Fernsehmonitor u. dgl.)
- Einbau von Schleusen
- Closed-Shop-Betrieb
- Entsprechende Ausgestaltung der Maßnahmen zur Objektsicherung (z. B. Spezialverglasung, Einbruchmeldesystem, Absicherung von Schächten, Geländebewachung)

3.2 Abgangskontrolle

3.21 Text der Anlage zum BDSG

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

3.22 Erläuterungen

3.221 Bei der Verarbeitung personenbezogener Daten tätige Personen:

Zu berücksichtigen sind sämtliche Personen, die für die in § 1 Abs. 2 Satz 1 BDSG genannten Personen oder Stellen bei der automatischen Datenverarbeitung tätig sind. Hierzu können gehören z. B. die unmittelbar in Rechenzentren und im Bereich der Verfahrensentwicklung und Programmierung Beschäftigten oder Personen, die zentral oder dezentral Daten erfassen oder verändern (Offline oder Online). Zur „Verarbeitung von Daten" siehe Nr. 3.124. Für Personen, die nicht bei der Datenverarbeitung tätig sind, jedoch Zugang zu Datenträgern haben, können gleichwohl Maßnahmen nach § 6 Abs. 1 BDSG in Betracht kommen.

3.222 Datenträger:

Siehe Nr. 3.026

3.223 Unbefugtes Entfernen:

Datenträger werden unbefugt entfernt, wenn sie aus dem durch die Befugnis abgedeckten Bereich herausgenommen werden.

3.23 Zielrichtung

Ziel der Abgangskontrolle ist es, mit Hilfe geeigneter Maßnahmen bei der Verarbeitung personenbezogener Daten tätige Personen an der unbefugten Entfernung von Datenträgern zu hindern. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.24 Verfahrensschritte

- Festlegung der Bereiche, in denen sich Datenträger befinden dürfen
- Festlegung der Personen, die aus diesen Bereichen befugt Datenträger entfernen dürfen
- Kontrolle der Entfernung von Datenträgern
- Absicherung der Bereiche, in denen sich Datenträger befinden

3.25 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)

- Feststellung befugter Personen
- Ausgabe von Datenträgern nur an autorisierte Personen (z. B. Auftragsquittung, Begleitpapier)
- Datenträgerverwaltung
- Lagerung der Datenträger in einem Sicherheitsbereich (Dateiarchiv)
- Bestandskontrollen
- Sicherheitsschränke
- Verbot der Mitnahme von Taschen und sonstigen Gepäckstücken in die Sicherheitsbereiche
- Kontrollierte Vernichtung von Datenträgern (z. B. Fehldrucke)
- Regelung der Anfertigung von Kopien

3.3 Speicherkontrolle

3.31 Text der Anlage zum BDSG

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

3.32 Erläuterungen

3.321 Eingabe in den Speicher:

Eingabe ist die Aufnahme von Daten in den Speicher eines Datenverarbeitungssystems (siehe Nr. 3.022).

Ein Speicher ist eine Funktionseinheit innerhalb eines Datenverarbeitungssystems, der Daten aufnimmt, aufbewahrt und abgibt (vgl. DIN 44 300).

Hierzu gehören sowohl der Hauptspeicher der Datenverarbeitungsanlage (siehe Nr. 3.021) als auch maschinell verarbeitbare Datenträger (siehe dazu Nr. 3.026), wenn und solange diese in ein Datenverarbeitungssystem integriert sind.

Im Sinne dieser Erläuterung ist zwischen Speicher und Datenträger zu unterscheiden. Eine Magnetplatte z. B. ist für sich allein nur Datenträger. Sobald sie in ein am Datenverarbeitungssystem angeschlossenes Magnetplattenlaufwerk eingelegt ist, wird sie zum Bestandteil des Speichers.

3.322 Kenntnisnahme, Veränderung, Löschung gespeicherter Daten:

„Kenntnisnahme" ist das unmittelbare oder mittelbare geistige Aufnehmen gespeicherter Daten.

Unter „Veränderung" und „Löschung" sind die in § 2 Abs. 2 Nr. 3 und 4 BDSG definierten Verarbeitungsphasen zu verstehen.

Die Kenntnisnahme, Veränderung oder Löschung kann unmittelbar über die Konsole oder ein Datenendgerät sowie mittelbar über maschinell verarbeitbare Datenträger erfolgen; die Veränderung oder Löschung kann auch durch Hinzufügen, Entfernen oder Austauschen einzelner solcher Datenträger geschehen.

3.323 Unbefugt:

Siehe Nr. 3.025, bezogen auf die Eingabe, Kenntnisnahme, Veränderung oder Löschung von Daten.

3.33 Zielrichtung

Ziel der Speicherkontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, daß personenbezogene Daten nur befugt gespeichert und gespeicherte

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

personenbezogene Daten nur befugt verwendet werden können. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.34 Verfahrensschritte
- Festlegung der Befugnis für die
  - Eingabe von Daten in Speicher
  - Kenntnisnahme gespeichter Daten
  - Veränderung gespeicherter Daten
  - Löschung gespeicherter Daten
- Legimitation der Befugten
- Absicherung der
  - Eingabe von Daten in Speicher
  - Kenntnisnahme gespeicherter Daten
  - Veränderung gespeicherter Daten
  - Löschung gespeicherter Daten

3.35 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)
- Einsatz von Benutzercodes für Dateien und Programme
- Einsatz von Verschlüsselungsroutinen für Dateien
- Differenzierte Zugriffsregelung (z. B. durch Segment-Zugriffssperren)
- Richtlinien für die Dateiorganisation
- Protokollierung der Dateibenutzung
- Besondere Kontrolle des Einsatzes von Hilfsprogrammen, soweit diese geeignet sind, Sicherungsmaßnahmen zu umgehen

3.4 Benutzerkontrolle

3.41 Text der Anlage zum BDSG

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

3.42 Erläuterungen

3.421 Datenverarbeitungssystem:
Siehe Nr. 3.022

3.422 Benutzung:
Siehe Nr. 3.023

3.423 Selbsttätige Einrichtungen:
Siehe Nr. 3.024

3.424 Übermittlung:
Unter „Übermitteln" ist zu verstehen die in § 2 Abs. 2 Nr. 2 BDSG definierte Phase der Datenverarbeitung in Verbindung mit der Definition des Dritten lt. § 2 Abs. 3 Nr. 2 BDSG.
Daraus ergibt sich z. B., daß der Datenaustausch innerhalb der speichernden Stelle von der Benutzerkontrolle nicht betroffen ist. Ferner ist nicht betroffen der Datenaustausch zwischen Auftraggeber und Auftragnehmer bei der Auftrags-Datenverarbeitung im Geltungsbereich des BDSG (vgl. aber Nr. 3.01 Absatz 2).

3.425 Unbefugte Personen:
Siehe Nr. 3.025, bezogen auf die Benutzung von Datenverarbeitungssystemen.

3.43 Zielrichtung
Ziel der Benutzerkontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, daß unbefugte Personen solche Datenverarbeitungssysteme benutzen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.44 Verfahrensschritte
- Festlegung der Benutzungsberechtigungen
- Legitimation der Benutzungsberechtigten
- Kontrolle der Benutzung von Datenverarbeitungssystemen
- Absicherung der Datenverarbeitungssysteme

3.45 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)
- Abschließbarkeit von Datenstationen
- Identifizierung eines Terminals und/oder eines Terminalbenutzers gegenüber dem DV-System (z. B. durch Ausweisleser)
- Vergabe und Sicherung von Identifizierungsschlüsseln
- Zuordnung einzelner Terminals und Identifizierungsmerkmale ausschließlich für bestimmte Funktionen
- Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals und Identifizierungsmerkmalen
- Auswertung von Protokollen
- Regelung der Benutzungsberechtigung

3.5 Zugriffskontrolle

3.51 Text der Anlage zum BDSG

„Es ist zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können."

3.52 Erläuterungen

3.521 Benutzung eines Datenverarbeitungssystems:
Siehe Nr. 3.023

3.522 Berechtigte:
Berechtigte sind Personen, bei denen der Zugriff auf Daten im Rahmen der ihnen übertragenden Aufgaben oder einer anderweitigen Ermächtigung liegt.

3.523 Selbsttätige Einrichtungen:
Siehe Nr. 3.024

3.524 Zugriff:
Zugriff ist die Einwirkung auf ein Datenverarbeitungssystem (siehe Nr. 3.022) mit der Möglichkeit der Kenntnisnahme, der Veränderung oder einer anderweitigen Verarbeitung oder Nutzung von Daten.

3.53 Zielrichtung
Die Maßnahmen müssen darauf gerichtet sein, daß durch selbsttätige Einrichtungen nur auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.54 Verfahrensschritte
- Festlegung der Zugriffsberechtigungen für den Zugriff auf Daten durch selbsttätige Einrichtungen
  - für Personen
  - für Datenbereiche
- Legitimation der Zugriffsberechtigten
- Kontrolle des Zugriffs
- Absicherung des über selbsttätige Einrichtungen erfolgenden Zugriffs

3.55 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)
- Zuordnung einzelner Terminals und Identifizierungsmerkmale ausschließlich für bestimmte Funktionen
- Funktionelle und/oder zeitlich beschränkte Nutzung von Terminals und Identifizierungsmerkmalen
- Datenstationen mit Funktionsberechtigungsschlüsseln
- Regelung der Zugriffsberechtigung
- Überprüfung der Berechtigung, maschinell z. B. durch Identifizierungsschlüssel
- Auswertung von Protokollen
- Ausweisleser am Terminal
- Zeitliche Begrenzung der Zugriffsmöglichkeit
- Teilzugriffsmöglichkeit auf Datenbestände und Funktionen

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

3.6 **Übermittlungskontrolle**

3.61 Text der Anlage zum BDSG

„Es ist zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können."

3.62 Erläuterungen

3.621 Überprüft und festgestellt werden kann:

Die Überprüfung und Feststellung muß nicht dauernd tatsächlich erfolgen, sondern sie muß möglich sein (z. B. anhand der Verfahrens- und Ablaufdokumentation).

3.622 Stellen:

Darunter ist jeder „Dritte" entsprechend der in § 2 Abs. 3 Nr. 2 BDSG gegebenen Definition zu verstehen.

3.623 Selbsttätige Einrichtungen:

Siehe Nr. 3.024

3.624 Übermittelt werden können:

Es kommt hier weder auf die tatsächliche, noch auf die theoretisch mögliche, sondern auf die nach der Verfahrenskonzeption vorgesehene Übermittlung (§ 2 Abs. 2 Nr. 2 BDSG) an.

3.63 Zielrichtung

Ziel der Übermittlungskontrolle ist es, mit Hilfe geeigneter Maßnahmen bei den durch selbsttätige Einrichtungen erfolgenden Datenübermittlungen die nach der Verfahrenskonzeption vorgesehenen Empfänger feststellen zu können. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.64 Verfahrensschritte

- Festlegung der Stellen, an die durch selbsttätige Einrichtungen Daten übermittelt werden können
- Dokumentation in der Weise, daß eine Feststellung der „Dritten" möglich ist

3.65 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)

- Dokumentation der Abruf- und Übermittlungsprogramme
- Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege (Konfiguration)

3.7 **Eingabekontrolle**

3.71 Text der Anlage zum BDSG

„Es ist zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind."

3.72 Erläuterungen

3.721 Nachträglich überprüft und festgestellt werden kann:

Die Überprüfung und Feststellung muß nicht dauernd tatsächlich erfolgen, sondern sie muß nach erfolgter Eingabe anhand von Unterlagen möglich sein. Die Protokollierung der einzelnen Eingaben wird demnach vom Gesetz für den Regelfall nicht vorgeschrieben. Es reicht vielmehr aus, wenn die näheren Umstände einer Eingabe z. B. wegen der Organisation des Verfahrens jederzeit rekonstruierbar sind. Die Nachweisfrist muß den Erfordernissen des Einzelfalles angemessen sein. Sonstige Aufbewahrungsvorschriften werden nicht berührt.

3.722 Zu welcher Zeit:

Der Zeitpunt der Dateneingabe muß in Abhängigkeit von der Verarbeitung bestimmbar sein. Dies kann durch Einzelnachweis oder aufgrund organisatorischer Regelungen geschehen.

3.723 Von wem:

Hiermit ist je nach Lage des Einzelfalles entweder eine einzelne Person oder eine Organisationseinheit gemeint. Im letzteren Falle muß sichergestellt sein, daß anhand der getroffenen organisatorischen Festlegungen die in Betracht kommenden Personen festgestellt oder der Personenkreis näher eingeengt werden können.

3.724 Datenverarbeitungssystem:

Siehe Nr. 3.022

3.725 Eingeben von Daten:

Eingabe ist jeder Vorgang in einem Datenverarbeitungssystem, mit dem das System Daten von außen her aufnimmt (vgl. DIN 44 300).

3.73 Zielrichtung

Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, daß nachträglich die näheren Umstände der Dateneingabe überprüft und festgestellt werden können. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.74 Verfahrensschritte

- Dokumentation der Eingabeverfahren mit der Möglichkeit der nachträglichen Überprüfung der erfolgten Dateneingaben

3.75 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)

- Nachweis der organisatorisch festgelegten Zuständigkeiten für die Eingabe
- Protokollierung von Eingaben

3.8 **Auftragskontrolle**

3.81 Text der Anlage zum BDSG

„Es ist zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können."

3.82 Erläuterungen

3.821 Auftragsverhältnis:

Welcher Art die Rechtsbeziehungen zwischen Auftraggeber und Auftragnehmer sind, ist unbeachtlich. Es kommen Auftragsverhältnisse jeglicher Art, wie z. B. Dienstleistungsverträge, Werkverträge oder gemischte Vertragsverhältnisse in Betracht.

Besondere Formvorschriften bestehen nicht.

3.822 Weisungen:

Zwischen Auftraggeber und Auftragnehmer muß eine – möglichst schriftliche – Regelung über die vom Auftragnehmer durchzuführende Datenverarbeitung bestehen.

3.83 Zielrichtung

Diese Anforderung verpflichtet den Auftragnehmer im Sinne des § 2 Abs. 3 Nr. 2 BDSG. Die Auftragskontrolle ist als Ergänzung der Vorschriften der §§ 8, 22 Abs. 2, 31 Abs. 2 und 37 BDSG anzusehen. Danach ist die Verarbeitung personenbezogener Daten in allen vier Phasen der Datenverarbeitung nur im Rahmen der Weisungen des Auftraggebers gestattet. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.84 Verfahrensschritte

- Eindeutige Vertragsgestaltung
- Kontrolle der Vertragsausführung

3.85 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)

- Sorgfältige Auswahl der Auftragnehmer
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Formalisierung der Auftragserteilung
- Kontrolle der Arbeitsergebnisse

3.9 **Transportkontrolle**

3.91 Text der Anlage zum BDSG

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

Ministerialblatt für das Land Nordrhein-Westfalen – Nr. 17 vom 22. März 1979

3.92 Erläuterungen

3.921 Transport entsprechender Datenträger:

Hiermit ist jeglicher Transport von Datenträgern (siehe Nr. 3.026) mit geschützten personenbezogenen Daten gemeint – und zwar sowohl der Transport innerhalb der speichernden Stelle als auch der Transport an Dritte, soweit die Datenträger den Dateibegriff von § 2 Abs. 3 Nr. 3 BDSG erfüllen. Beim Transport von Datenträgern, die nicht den Dateibegriff erfüllen, kommen Maßnahmen nach § 6 Abs. 1 BDSG in Betracht, um die mißbräuchliche Kenntnisnahme von Daten zu verhindern.

3.922 Übermittlung von Daten:

Siehe Nr. 3.424. Daraus und aus Nr. 3.921 ergibt sich, daß der Datenaustausch innerhalb der speichernden Stelle und der Datenaustausch zwischen Auftraggeber und Auftragnehmer bei der Auftrags-Datenverarbeitung im Geltungsbereich des BDSG von der Transportkontrolle nicht betroffen sind, wenn die Übertragung von Daten auf Übertragungsleitungen und nicht mit Datenträgern, die den Dateibegriff erfüllen, erfolgt; vgl. aber Nr. 3.01 Abs. 2.

3.923 Lesen, Verändern, Löschen von Daten:

„Lesen" ist die Kenntnisnahme (siehe Nr. 3.322) gespeicherter Daten.

Zum „Verändern" und „Löschen" von Daten siehe die unter Nr. 3.322 zu diesen Begriffen gegebenen Erläuterungen.

3.924 Unbefugt:

Siehe Nr. 3.025, bezogen aus das Lesen, Verändern oder Löschen von Daten.

3.93 Zielrichtung

Ziel der Transportkontrolle ist es, durch geeignete Maßnahmen personenbezogene Daten auch bei der Übermittlung und dem Transport zu sichern. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.94 Verfahrensschritte

- Festlegung der zur Übermittlung bzw. zum Transport Befugten
- Legimitation der Berechtigten
- Festlegung der Wege und Verfahren
- Absicherung der Übermittlung bzw. des Transports

3.95 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)

- Verpackungs- und Versandvorschriften (Versandart z. B. in verschlossenen Behältnissen)
- Verschlüsselung
- Direktabholung, Kurierdienst, Transportbegleitung
- Plausibilitätsprüfung
- Vollständigkeits- und Richtigkeitsprüfung

3.10 **Organisationskontrolle**

3.10.1 Text der Anlage zum BDSG

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

3.10.2 Zielrichtung

Ziel der Organisationskontrolle ist es, die technischen und organisatorischen Maßnahmen zu unterstützen, zu ergänzen und aufeinander abzustimmen. Um dieses Ziel zu erreichen, kommen etwa folgende Verfahrensschritte in Betracht:

3.10.3 Verfahrensschritte

- Festlegung der Funktionen, der Zuständigkeiten und Verantwortung bei der Datenverarbeitung
- Regelungen zur ordnungsgemäßen und sicheren Abwicklung der automatisierten Datenverarbeitungsaufgaben
- Überwachung der Einhaltung der Regelungen
- Prüfung der Wirksamkeit der Regelungen und Maßnahmen und permanente Anpassung

3.10.4 Beispiele für Maßnahmen (siehe dazu Nr. 3.01)

- Funktionstrennung (z. B. 4-Augen-Prinzip, Closed-Shop-Betrieb)
- Richtlinien und Arbeitsanweisungen
- Stellenbeschreibung
- Verfahrensdokumentation
- Regelungen zur Programmierung
- Regelungen zur System- und Programmprüfung
- Abstimm- und Kontrollsystem
- Auflagen zur sicheren Behandlung und Aufbewahrung von Eingabelisten und Ausdrucken

Im Einvernehmen mit dem Ministerpräsidenten, Minister für Wirtschaft, Mittelstand und Verkehr, Finanzminister, Justizminister, Minister für Wissenschaft und Forschung, Kultusminister, Minister für Ernährung, Landwirtschaft und Forsten, Minister für Arbeit, Gesundheit und Soziales, Minister für Bundesangelegenheiten.

– MBl. NW. 1979 S. 362.