LANDTAG NORDRHEIN-WESTFALEN **Drucksache 10/1565**

10. Wahlperiode

05. 01. 1987

Gesetzentwurf

der Landesregierung

Gesetz zur Fortentwicklung des Datenschutzes (GFD)

A Problem

Nach der grundlegenden Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65, 1) zum Volkszählungsgesetz wird – insbesondere unter den Bedingungen der modernen Datenverarbeitung – der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Übermittlung und Nutzung seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikels 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz umfaßt. Dieses Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). Die Entscheidung des Bundesverfassungsgerichts bestätigt zugleich die Intentionen des Artikels 4 Absatz 2 der Landesverfassung Nordrhein-Westfalen, der überall dort, wo der Umgang mit personenbezogenen Daten als Eingriff in die Persönlichkeitssphäre des einzelnen zu werten ist, eine diesen Eingriff legitimierende Norm fordert. Die Vorschriften des Landes über den Umgang mit personenbezogenen Daten in der öffentlichen Verwaltung sind, soweit erforderlich, entsprechend anzupassen; dabei kommt der Novellierung des allgemeinen Datenschutzrechts besondere Bedeutung zu.

B Lösung

Der Gesetzentwurf zieht in einem wesentlichen Schritt die notwendigen Konsequenzen aus dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz. Er verfolgt schwerpunktmäßig das Ziel, das für die Landes- und Kommunalverwaltung in Nordrhein-Westfalen geltende Datenschutzgesetz im Interesse der betroffenen Bürger neuzufassen und auszubauen. Gleichzeitig wird damit auch ein allgemeines Ausführungsgesetz zu Artikel 4 Absatz 2 der Landesverfassung geschaffen. Der Gesetzentwurf beabsichtigt in Artikel 1, eine umfassend angelegte Konzeption für den Umgang mit personenbezogenen Daten in der öffentlichen Verwaltung zu verwirklichen, die auch für die darüber hinaus notwendigen bereichsspezifischen Datenschutzregelungen Leitfunktionen übernehmen soll. Die Datenschutzveröffentlichungsverordnung soll aufgehoben werden (Artikel 2). Parallel dazu sollen Vorschriften des Verwaltungsverfahrens- und des Meldegesetzes geändert werden, soweit diese für den Umgang mit personenbezogenen Daten von Bedeutung sind (Artikel 3 und 4). Bei dieser Gelegenheit erfolgt auch eine Klarstellung bezüglich der Kontrollzuständigkeiten im Rahmen des Gesetzes über den „Westdeutschen Rundfunk Köln" (Art. 5).

C Alternative

Keine. Eine unveränderte Beibehaltung des Datenschutzgesetzes Nordrhein-Westfalen sowie der übrigen vorgenannten Vorschriften kommt wegen der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 und des Artikels 4 Absatz 2 der Landesverfassung, der Zunahme der Informationsverarbeitung im öffentlichen Bereich und des Aufkommens neuer Informationstechniken nicht in Betracht.

D Kosten

Die Sicherung des informationellen Selbstbestimmungsrechts im Rahmen des Datenschutzes ist ein bedeutsamer Aspekt der rechtmäßigen Aufgabenerfüllung durch die öffentliche Verwaltung. Die bei der Durchführung einer solchen Querschnittsaufgabe für die Landes- und Kommunalverwaltung anfallen-

Datum des Originals: 25. 11. 1986 / Ausgegeben: 22. 01. 1987

Die Veröffentlichungen des Landtags sind fortlaufend oder auch einzeln gegen eine Schutzgebühr beim Archiv des Landtags Nordrhein-Westfalen, 4000 Düsseldorf 1, Postfach 1143, Telefon (0211) 884439, zu beziehen.

den Kosten sind Bestandteil der allgemeinen Verwaltungskosten und insoweit abgedeckt. Kosten für den Datenschutz sind gesondert nicht abschätzbar; sie richten sich nach der jeweiligen Verwaltungsaufgabe und den besonderen Verhältnissen des Aufgabenträgers. Dies gilt um so mehr, als der vorliegende Gesetzentwurf nur eine teilweise Neustrukturierung bereits geltender datenschutzrechtlicher Regelungen vorsieht.

E Zuständigkeit

Zuständig ist der Innenminister, beteiligt sind alle Ressorts.

F Auswirkungen auf die kommunale Selbstverwaltung

Die Zuständigkeiten und der verfassungsrechtlich garantierte Bereich der kommunalen Selbstverwaltung werden durch den Gesetzentwurf nicht berührt.

Gesetz zur Fortentwicklung des Datenschutzes (GFD)

Inhaltsübersicht

Gesetz zur Fortentwicklung des Datenschutzes (GFD)

Artikel 1

Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen – DSG NW –)

Inhaltsübersicht

Auszug aus den geltenden Gesetzesbestimmungen

Gesetz zum Schutz vor Mißbrauch pesonenbezogener Daten bei der Datenverarbeitung (Datenschutzgesetz Nordrhein-Westfalen – DSG NW –)

Inhaltsübersicht

Erster Teil

Allgemeiner Datenschutz

Erster Abschnitt

Allgemeine Bestimmungen

§ 1

Aufgabe

Aufgabe dieses Gesetzes ist es,

1. den einzelnen davor zu schützen, daß er durch die Verarbeitung personenbezogener Daten durch öffentliche Stellen in unzulässiger Weise in seinem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht),
2. das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes, und die Zuständigkeitsabgrenzung zwischen den Organen der kommunalen Selbstverwaltung sowie zwischen der staatlichen Verwaltung und der kommunalen Selbstverwaltung vor einer Gefährdung durch die automatisierte Datenverarbeitung zu bewahren.

§ 2

Anwendungsbereich

(1) Dieses Gesetz gilt für die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen (öffentliche Stellen), soweit diese personenbezogene Daten in oder aus Dateien oder Akten verarbeiten; für den Landtag sowie für die Gerichte und die Behörden der Staatsanwaltschaft gilt dieses Gesetz nur, soweit sie Verwaltungsaufgaben erledigen. Für die Ausübung des Gnadenrechts findet das Gesetz keine Anwendung.

Erster Abschnitt

Allgemeine Bestimmungen

§ 1

Aufgabe und Gegenstand des Datenschutzes

(1) Aufgabe des Datenschutzes ist es,

1. den Bürger durch Verhinderung des Mißbrauchs bei der Verarbeitung (Speicherung, Übermittlung, Veränderung und Löschung) personenbezogener Daten zu schützen und einer Beeinträchtigung schutzwürdiger Belange entgegenzuwirken,

2. das auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landes, und die Zuständigkeitsabgrenzung der Organe der kommunalen Selbstverwaltung untereinander und zueinander, vor einer Veränderung infolge der automatisierten Datenverarbeitung zu bewahren.

(2) Dieses Gesetz schützt personenbezogene Daten, die von den Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, den Gemeinden und Gemeindeverbänden sowie den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. Für die Gerichte und Behörden der Staatsanwaltschaft gilt dieses nur, wenn sie Verwaltungsaufgaben erledigen. Für personenbezogene Daten, die nicht zur Übermittlung an Dritte bestimmt sind und in nicht automatisierten Verfahren verarbeitet werden, gilt von den Vorschriften dieses Gesetzes nur § 6, soweit er die Verpflichtung enthält, technische und organisatorische Maßnahmen zum Schutz dieser Daten gegenüber Dritten zu treffen.

(2) Von den Vorschriften dieses Gesetzes gelten nur die Vorschriften des Zweiten Teils sowie die §§ 8 und 28 bis 31 dieses Gesetzes, soweit

1. wirtschaftliche Unternehmen der Gemeinden oder Gemeindeverbände ohne eigene Rechtspersönlichkeit (Eigenbetriebe),
2. öffentliche Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe oder nach der Gemeindekrankenhausbetriebsverordnung geführt werden,
3. der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen,

personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Im übrigen sind mit Ausnahme der §§ 28 bis 30 sowie der §§ 38 bis 40 die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anzuwenden.

Unbeschadet der Regelung des Absatzes 1 Satz 1 gelten Schulen der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, als öffentliche Stellen im Sinne dieses Gesetzes.

(3) Dieses Gesetz schützt personenbezogene Daten nicht, die durch den Rundfunk ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden; § 6 Abs. 1 bleibt unberührt.

§ 18

Geltungsbereich

Von den Vorschriften dieses Gesetzes gelten anstelle der §§ 10 bis 17 die Vorschriften dieses Abschnitts, soweit

1. *wirtschaftliche Unternehmen der Gemeinden oder Gemeindeverbände ohne eigene Rechtspersönlichkeit (Eigenbetriebe) oder öffentliche Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden, personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer wirtschaftlichen Zwecke oder Ziele verarbeiten;*
2. *der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen, personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten.*

(3) Soweit besondere Rechtsvorschriften auf die Verarbeitung personenbezogener Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

§ 37

Weitergeltende Vorschriften

Soweit besondere Rechtsvorschriften des Landes auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor.

§ 3

Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten.

Im einzelnen ist

1. Erheben (Erhebung) das Beschaffen von Daten über den Betroffenen,
2. Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,

§ 2

Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Im Sinne dieses Gesetzes ist

1. *Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung,*
2. *Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte in der Weise, daß die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden,*
3. *Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,*

4. Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, daß die Daten durch die datenverarbeitende Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden oder daß der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten abruft,
5. Sperren (Sperrung) das Verhindern weiterer Verarbeitung gespeicherter Daten,
6. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten,
7. Nutzen (Nutzung) jede sonstige Verwendung personenbezogener Daten, ungeachtet der dabei angewendeten Verfahren.

(3) Dritter ist jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Stellen, die als Auftragnehmer (§ 11) im Geltungsbereich des Grundgesetzes tätig werden.

(4) Eine Datei ist

a) eine Sammlung von Daten, die ohne Rücksicht auf die Art der Speicherung durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder

b) eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht-automatisierte Datei).

(5) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

§ 4

Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

a) dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder

b) der Betroffene eingewilligt hat.

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung über die Empfänger der Daten aufzuklären; er ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann.

4. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten, ungeachtet der dabei angewendeten Verfahren.

(3) Im Sinne dieses Gesetzes ist

1. *speichernde Stelle jede der in § 1 Abs. 2 genannten Stellen, die Daten für sich selbst speichert oder durch andere speichern läßt,*
2. *Dritter jede Person oder Stelle außerhalb der speichernden Stelle, ausgenommen der Betroffene oder diejenigen Stellen, die in den Fällen der Nummer 1 im Geltungsbereich des Grundgesetzes im Auftrag tätig werden,*
3. *eine Datei eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren; nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.*

§ 3

Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten, die von diesem Gesetz geschützt werden, ist in jeder ihrer in § 1 Abs. 1 genannten Phasen nur zulässig, wenn

1. *dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder*
2. *der Betroffene eingewilligt hat.*

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist; wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen.

Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären.

§ 5

Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. **Auskunft, Einsicht in Akten (§ 18),**
2. **Berichtigung, Sperrung oder Löschung (§ 19),**
3. **Schadensersatz (§ 20),**
4. **Anrufung des Landesbeauftragten für den Datenschutz (§ 25 Abs. 1),**
5. **Auskunft aus dem beim Landesbeauftragten für den Datenschutz geführten Dateienregister (§ 23 Abs. 2).**

Diese Rechte können auch durch die Einwilligung des Betroffenen nicht ausgeschlossen oder beschränkt werden.

§ 4

Rechte des Betroffenen

(1) Jeder hat nach Maßgabe des Gesetzes ein Recht auf

1. *Auskunft über die zu seiner Person gespeicherten Daten (§§ 16, 22),*
2. *Berichtigung der zu seiner Person gespeicherten Daten, wenn sie unrichtig sind (§§ 17, 23),*
3. *Sperrung der zu seiner Person gespeicherten Daten, wenn sich weder deren Richtigkeit noch deren Unrichtigkeit feststellen läßt oder nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung (§§ 17, 23),*
4. *Löschung der zu seiner Person gespeicherten Daten, wenn ihre Speicherung unzulässig war oder – wahlweise neben dem Recht auf Sperrung – nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung (§§ 17, 23),*
5. *Einsicht in das gemäß § 27 Abs. 1 geführte Register,*
6. *Unterlassung oder Beseitigung einer Beeinträchtigung schutzwürdiger Belange, wenn diese nach Berichtigung, Sperrung oder Löschung andauert; der Anspruch richtet sich gegen den Träger der öffentlichen Stelle, von der die Beeinträchtigung ausgeht,*
7. *Anrufung des Landesbeauftragten für den Datenschutz (§ 29).*

§ 6

Datengeheimnis

Denjenigen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren; dies gilt auch nach Beendigung ihrer Tätigkeit.

§ 5

Datengeheimnis

(1) Den im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Stellen bei der Datenverarbeitung beschäftigten Personen ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen.

(2) Diese Personen sind bei der Aufnahme ihrer Tätigkeit nach Maßgabe von Absatz 1 zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

§ 7

Sicherstellung des Datenschutzes

Die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen haben jeweils für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

§ 8

Durchführung des Datenschutzes

Die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen haben jeweils für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen und für die

Beachtung der Grundsätze des § 11 Abs. 1 auch dann zu sorgen, wenn personenbezogene Daten innerhalb einer Behörde, Einrichtung oder sonstigen öffentlichen Stelle weitergegeben oder zur Einsichtnahme namentlich zum Abruf bereitgehalten werden. Sie haben insbesondere dafür zu sorgen, daß

1. *eine Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren Empfänger oder Empfängergruppen und die Voraussetzungen für ihre Übermittlung geführt und*
2. *die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.*

§ 8

Dateibeschreibung

(1) Die speichernde Stelle ist verpflichtet, in einer Dateibeschreibung schriftlich festzulegen:

1. die Bezeichnung der Datei und ihre Zweckbestimmung,
2. die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Verarbeitung,
3. den Kreis der Betroffenen,
4. die Art regelmäßig zu übermittelnder Daten, deren Empfänger sowie die Herkunft regelmäßig empfangener Daten,
5. Fristen für die Sperrung und Löschung der Daten,
6. die technischen und organisatorischen Maßnahmen gemäß § 10,
7. bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte, die Stellen, bei denen sie aufgestellt sind sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.

(2) Absatz 1 findet keine Anwendung auf nicht automatisierte Dateien, aus denen keine Daten an Dritte übermittelt werden, sowie auf Dateien, die bei automatisierter Verarbeitung ausschließlich aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden.

§ 9

Automatisiertes Abrufverfahren und regelmäßige Datenübermittlungen

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist.

(2) Die Minister werden ermächtigt, für die Behörden und Einrichtungen ihres Geschäftsbereichs automatisierte Abrufverfahren durch Rechtsverordnung einzuführen. Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. Die Datenempfänger, die Datenart und der Zweck des Abrufs sind festzulegen. Der Landesbeauftragte für den Datenschutz ist zu unterrichten.

(3) Die am Abrufverfahren beteiligten Stellen haben die nach § 10 erforderlichen Maßnahmen zu treffen.

(4) Für die Einrichtung automatisierter Abrufverfahren innerhalb einer öffentlichen Stelle gelten Absatz 2 Satz 2 und 3 sowie Absatz 3 entsprechend.

(5) Personenbezogene Daten dürfen für Stellen außerhalb des öffentlichen Bereichs zum automatisierten Abruf nicht bereitgehalten werden; dies gilt nicht für den Betroffenen.

(6) Die Absätze 1 bis 5 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offenstehen oder deren Veröffentlichung zulässig wäre.

(7) Die Absätze 1 bis 6 sind auf die Zulassung regelmäßiger Datenübermittlungen entsprechend anzuwenden.

§ 10

Technische und organisatorische Maßnahmen

(1) Öffentliche Stellen, die selbst oder im Auftrag einer anderen öffentlichen Stelle personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Verarbeitung der Daten sicherzustellen. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 6

Technische und organisatorische Maßnahmen

(1) Wer im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Stellen personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Die Landesregierung wird ermächtigt, durch Rechtsverordnung, die im Einvernehmen mit dem zuständigen Landtagsausschuß ergeht, die in der Anlage genannten Anforderungen nach dem jeweiligen Stand der Technik und Organisation forzuschreiben. Stand der Technik und Organisation im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Gewährleistung der Durchführung dieses Gesetzes gesichert erscheinen läßt. Bei der Bestimmung des Standes der Technik und Organisation sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg im Betrieb erprobt worden sind.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu den Datenverarbeitungsanlagen zu verwehren (Zugangskontrolle),
2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten zu verhindern (Speicherkontrolle),
4. zu verhindern, daß Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit an wen durch Einrichtungen zur Datenübertragung übermittelt worden sind (Übermittlungskontrolle),
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, daß Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu gewährleisten, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(3) Werden personenbezogene Daten in nichtautomatisierten Dateien oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

Anlage

zu § 6 Abs. 1 Satz 1

Werden personenbezogene Daten automatisch verarbeitet, sind zur Ausführung der Vorschriften dieses Gesetzes Maßnahmen zu treffen die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. *Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),*
2. *Personen, die bei der Verarbeitung personenbezogener Daten tätig sind, daran zu hindern, daß sie Datenträger unbefugt entfernen (Abgangskontrolle),*
3. *die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),*
4. *die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern (Benutzerkontrolle),*
5. *zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),*
6. *zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können (Übermittlungskontrolle),*
7. *zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),*
8. *zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),*
9. *zu gewährleisten, daß bei der Übermittlung personenbezogener Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können (Transportkontrolle),*
10. *die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).*

§ 11

Verarbeitung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag einer öffentlichen Stelle verarbeitet, bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftraggeber ist speichernde Stelle im Sinne dieses Gesetzes; die in § 5 genannten Rechte sind ihm gegenüber geltend zu machen. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die Gewährleistung der nach § 10 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

(2) Soweit das Landesamt für Datenverarbeitung und Statistik (Landesdatenverarbeitungszentrale), die Gemeinsamen Gebietsrechenzentren, die Fachrechenzentren, die Hochschulrechenzentren und die kommunalen Datenverarbeitungseinrichtungen personenbezogene Daten im Auftrag öffentlicher Stellen verarbeiten, gelten für sie außer §§ 6 und 10 auch § 22 und §§ 24 bis 26 dieses Gesetzes unmittelbar.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet sicherzustellen, daß der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft. Bei einer Auftragsdurchführung außerhalb des Geltungsbereichs dieses Gesetzes ist die zuständige Datenschutzkontrollbehörde zu unterrichten.

Zweiter Abschnitt

Rechtsgrundlagen der Datenverarbeitung

§ 12

Erhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist. Durch die Art und Weise der Erhebung darf das allgemeine Persönlichkeitsrecht des Betroffenen nicht beeinträchtigt werden. Personenbezogene Daten sind beim Betroffenen mit seiner Kenntnis zu erheben; bei anderen Stellen oder Personen dürfen sie nur unter den Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstaben a bis h erhoben werden.

§ 7

Verarbeitung personenbezogener Daten im Auftrag

(1) Die Vorschriften dieses Gesetzes gelten für die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen auch insoweit, als personenbezogene Daten in deren Auftrag durch andere Personen oder Stellen verarbeitet werden. Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, sicherzustellen, daß der Auftragnehmer die Bestimmungen dieses Gesetzes beachtet und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

(2) Für das Landesamt für Datenverarbeitung und Statistik (Landesdatenverarbeitungszentrale), die Gemeinsamen Gebietsrechenzentren, die Fachrechenzentren, die Hochschulrechenzentren und die Kommunalen Datenverarbeitungszentralen gelten, soweit sie personenbezogene Daten im Auftrag der in § 1 Abs. 2 genannten Stellen verarbeiten, von den Vorschriften dieses Gesetzes nur die §§ 1 bis 9 und 24 bis 31. Das Landesamt für Datenverarbeitung und Statistik (Landesdatenverarbeitungszentrale), die Gemeinsamen Gebietsrechenzentren, die Fachrechenzentren, die Hochschulrechenzentren und die Kommunalen Datenverarbeitungszentralen, in denen die in § 1 Abs. 2 genannten Stellen Datenverarbeitungsaufgaben erledigen lassen, sind bei der Verarbeitung personenbezogener Daten in jeder ihrer in § 1 Abs. 1 genannten Phasen an die Weisung ihrer Auftraggeber gebunden.

Zweiter Abschnitt

Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen

§ 10

Datenspeicherung und -veränderung

(1) Das Speichern und das Verändern personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist.

(2) Werden Daten beim Betroffenen erhoben, so ist er über den Verwendungszweck aufzuklären. Werden die Daten auf Grund einer Rechtsvorschrift erhoben, so ist der Betroffene in geeigneter Weise über diese aufzuklären. Soweit eine Auskunftspflicht besteht oder die Angaben Voraussetzung für die Gewährung von Rechtsvorteilen sind, ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

(2) Werden Daten beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, dann ist er auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Dem Betroffenen dürfen aus einer Verweigerung der Einwilligung keine Rechtsnachteile entstehen.

(3) Werden Daten bei einer dritten Person oder einer nicht-öffentlichen Stelle erhoben, so ist diese auf Verlangen über den Verwendungszweck aufzuklären. Soweit eine Auskunftspflicht besteht, ist sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 13

Zweckbindung bei Speicherung, Veränderung und Nutzung

(1) Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Die Daten dürfen nur für Zwecke weiterverarbeitet werden, für die sie erhoben worden sind. Daten, von denen die Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben oder erstmals gespeichert worden sind, ist dies nur zulässig, wenn

a) eine Rechtsvorschrift dies erlaubt oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt,

b) der Betroffene eingewilligt hat,

c) Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

d) es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,

e) offensichtlich ist, daß es im Interesse des Betroffenen liegt und dieser in Kenntnis des anderen Zwecks seine Einwilligung erteilen würde,

f) sie aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das Interesse des Betroffenen an dem Ausschluß der Speicherung oder einer Veröffentlichung der gespeicherten Daten offensichtlich überwiegt,

g) es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,

h) sie zu Zwecken einer öffentlichen Auszeichnung des Betroffenen erforderlich ist oder

i) es zur Verfolgung von Straftaten oder Odnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder zur Vollstreckung von Bußgeldentscheidungen oder zur Erfüllung eines gerichtlichen Auskunftsersuchens erforderlich ist.

Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, findet Satz 1 Buchstaben c bis i keine Anwendung.

(3) Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Zulässig ist auch die Verarbeitung zu Ausbildungs- und Prüfungszwekken, soweit nicht berechtigte Interessen des Betroffenen an der Geheimhaltung der Daten offensichtlich überwiegen.

§ 14

Übermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Voraussetzungen des § 13 Abs. 1 Satz 2 oder Satz 3 oder des Absatzes 2 Satz 1 vorliegen, sowie zur Wahrnehmung von Aufgaben nach § 13 Abs. 3. Die Übermittlung ist ferner zulässig, soweit es zur Entscheidung in einem Verwaltungsverfahren der Beteiligung mehrerer öffentlicher Stellen bedarf.

(2) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(3) Die Verantwortung für die Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Grund eines Ersuchens des Empfängers, hat die übermittelnde Stelle lediglich zu prüfen,

§ 11

Datenübermittlung an Behörden und sonstige öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis (§ 45 Satz 2 Nr. 1 Satz 3 des Bundesdatenschutzgesetzes vom 27. Januar 1977, BGBl. I S. 201) und sind sie der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die übermittelnde Stelle erhalten hat.

ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlaß besteht; der Empfänger hat der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch automatisierten Abruf (§ 9), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs der Empfänger.

(4) Der Empfänger darf die übermittelten Daten nur für die Zwecke verarbeiten, zu deren Erfüllung sie ihm übermittelt worden sind; § 13 Abs. 2 findet entsprechende Anwendung.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 15

Übermittlung an öffentlich-rechtliche Religionsgesellschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an öffentliche Stellen zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen sind.

§ 16

Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

a) sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen des § 13 Abs. 1 vorliegen,

b) die Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstaben a, b, d, f oder g vorliegen,

c) der Auskunftsbegehrende ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, daß das Geheimhaltungsinteresse des Betroffenen überwiegt oder

d) sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und der Betroffene in diesen Fällen der Datenübermittlung nicht widersprochen hat.

In den Fällen des Satzes 1 Buchstabe d ist der Betroffene über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten.

(2) Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an Behörden und sonstige öffentliche Stellen zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

§ 13

Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen und andere Stellen als die in § 11 bezeichneten ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist oder soweit der Empfänger ein berechtigtes Ineresse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis (§ 45 Satz 2 Nr. 1, Satz 3 Bundesdatenschutzgesetz) und sind sie der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß die gleichen Voraussetzungen gegeben sind, unter denen sie die zur Verschwiegenheit verpflichtete Person übermitteln dürfte. Für die Übermittlung an Behörden oder sonstige Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen finden die Sätze 1 und 2 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen Anwendung.

(2) Der Empfänger darf die übermittelten Daten nur für die Zwecke verarbeiten, zu denen sie ihm übermittelt wurden.

§ 17

Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes

Eine Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen ist nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen zulässig. Eine Übermittlung darf auch erfolgen, wenn die Voraussetzungen des § 14 Abs. 1 Satz 1 oder des § 16 Abs. 1 erfüllt sind und im Empfängerland gleichwertige Datenschutzregelungen gelten. Die Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck dieses oder eines anderen Gesetzes im Geltungsbereich des Grundgesetzes verstoßen würde.

Dritter Abschnitt

Rechte des Betroffenen

§ 18

Auskunft, Einsicht in Akten

(1) Dem Betroffenen ist von der speichernden Stelle auf Antrag unentgeltlich Auskunft zu erteilen über

1. die zu seiner Person gespeicherte Daten,
2. den Zweck und die Rechtsgrundlage der Speicherung sowie
3. die Herkunft der Daten und die Empfänger von Übermittlungen.

Dies gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(2) Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen; sind die Daten in Akten gespeichert, ist dem Betroffenen auf Verlangen Einsicht zu gewähren. Auskunft aus Akten oder Akteneinsicht sind zu gewähren, soweit der Betroffene Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen, und soweit sich aus § 29 des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen nichts anderes ergibt.

(3) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht entfällt, soweit

(2) Der Empfänger darf die übermittelten Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt wurden.

§ 16

Auskunft an den Betroffenen

(1) Dem Betroffenen ist von der speichernden Stelle auf Antrag Auskunft über die zu seiner Person gespeicherten Daten und die Stellen, denen Daten regelmäßig übermittelt werden, zu erteilen. In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht in den Fällen des § 15 Abs. 2 Nrn. 1 und 2.

(3) Die Auskunftserteilung unterbleibt, soweit

1. *die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,*
2. *die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,*
3. *die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen einer dritten Person geheimgehalten werden müssen,*
4. *die Auskunft sich auf die Übermittlung personenbezogener Daten an die in § 15 Abs. 2 Nr. 1 dieses Gesetzes und in § 12 Abs. 2 Nr. 1 Bundesdatenschutzgesetz genannten Behörden bezieht.*

a) dies die ordnungsgemäße Erfüllung der Aufgaben der speichernden Stelle gefährden würde,

b) dies die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

c) die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(4) Einer Begründung für die Auskunftsverweigerung bedarf es nur dann nicht, wenn durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen.

(5) Bezieht sich die Auskunftserteilung oder die Akteneinsicht auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, sowie von den in § 12 Abs. 2 Nr. 1 Bundesdatenschutzgesetz genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Für die Versagung der Zustimmung gelten, soweit dieses Gesetz auf die genannten Behörden Anwendung findet, die Absätze 3 und 4 entsprechend.

(6) Werden Auskunft oder Akteneinsicht nicht gewährt, ist der Betroffene darauf hinzuweisen, daß er sich an den Landesbeauftragten für den Datenschutz wenden kann.

§ 19

Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten in nicht automatisierten Dateien oder in Akten zu berichtigen, so ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind.

(2) Personenbezogene Daten sind zu sperren, wenn

a) ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt,

b) der Betroffene an Stelle der Löschung nach Absatz 3 Satz 1 Buchstabe a die Sperrung verlangt,

(4) Das Gebührengesetz für das Land Nordrhein-Westfalen (GebG NW) vom 23. November 1971 (GV.NW. S. 354) findet mit der Maßgabe Anwendung, daß

1. Gebühren höchstens bis zur Deckung des unmittelbar auf Amtshandlungen dieser Art entfallenden Verwaltungsaufwandes erhoben werden,

2. Ausnahmen von der Gebührenpflicht durch die Gebührenordnung in den Fällen vorzusehen sind, in denen durch besondere Umstände die Annahme gerechtfertigt wird, daß personenbezogene Daten unrichtig oder unzulässig gespeichert weden, oder in denen die Auskunft zur Berichtigung oder Löschung gespeicherter personenbezogener Daten geführt hat.

§ 17

Berichtigung, Sperrung und Löschung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Sie sind ferner zu sperren, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

Gesperrte Daten sind mit einem ensprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet, insbesondere übermittelt, oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen in überwiegenden

c) die weitere Speicherung im Interesse des Betroffenen geboten ist,

d) sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

In den Fällen nach Satz 1 Buchstabe c sind die Gründe aufzuzeichnen. Bei automatisierten Dateien ist die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen; im übrigen ist ein entsprechender Vermerk anzubringen. Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr weiterverarbeitet werden, es sei denn, daß dies zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene eingewilligt hat.

Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene in die Nutzung eingewiligt hat.

(3) Personenbezogene Daten sind zu löschen, wenn

a) ihre Speicherung unzulässig ist oder

b) ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Satz 1 Buchstabe b nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist; soweit hiernach eine Löschung nicht in Betracht kommt, sind die personenbezogenen Daten auf Antrag des Betroffenen zu sperren.

(3) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig war oder wenn es in den Fällen des Absatzes 2 Satz 2 der Betroffene verlangt.

(4) Abgesehen von den Fällen des Absatzes 3 Satz 1 Buchstabe a ist von einer Löschung abzusehen, soweit die gespeicherten Daten aufgrund von Rechtsvorschriften einem Archiv zur Übernahme anzubieten sind.

(4) Von der Berichtigung gemäß Absatz 1 sowie von der Sperrung gemäß Absatz 2 Satz 1 und der Löschung gemäß Absatz 3 Satz 2 sind unverzüglich die Stellen zu verständigen, denen die Daten im Ramen regelmäßiger Datenübermittlung übermittelt wurden; im übrigen liegt die Verständigung im pflichtgemäßen Ermessen.

(5) Über die Berichtigung unrichtiger Daten, die Sperrung bestrittener Daten und die Löschung oder Sperrung unzulässig gespeicherter Daten sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt worden sind. Die Unterrichtung kann unterbleiben, wenn sie einen erheblichen Aufwand erfordern würde und nachteilige Folgen für den Betroffenen nicht zu befürchten sind.

(5) Die Landesregierung wird ermächtigt, durch Rechtsverordnung Fristen festzulegen, nach deren Ablauf die in § 1 Abs. 2 genannten Stellen zur Löschung oder Sperrung gespeicherter Daten verpflichtet sind.

§ 20

Schadensersatz

(1) Wird dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt, so ist ihm der Träger der datenverarbeitenden Stelle unabhängig von einem Verschulden zum Schadensersatz verpflichtet. In schweren Fäl-

§ 4

Rechte des Betroffenen

(2) Wird der Betroffene durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder durch unrichtige Datenverarbeitung in seinen schutzwürdigen Belangen beeinträchtigt, so hat ihm die Stelle (§ 1 Abs. 2), die die Datenverarbeitung betreibt, den daraus entstehenden Schaden zu ersetzen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende

len kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 500000 Deutsche Mark.

(2) Auf eine schuldhafte Mitverursachung des Schadens durch den Betroffenen und die Verjährung des Entschädigungsanspruchs sind die §§ 254, 839 Abs. 3 und § 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(3) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

Ereignis bis zu einem Betrag von 250 000 DM. Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

Zweiter Teil

Landesbeauftragter für den Datenschutz

Vierter Abschnitt

Landesbeauftragter für den Datenschutz

§ 21

Berufung und Rechtsstellung

(1) Der Landtag wählt auf Vorschlag der Landesregierung einen Landesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Dieser muß die Befähigung zum Richteramt oder zum höheren Dienst haben und die zur Erfüllung seiner Aufgaben erforderliche Fachkunde besitzen.

(2) Der Landesbeauftragte für den Datenschutz wird jeweils auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen.

(3) Der Landesbeauftragte für den Datenschutz ist dem Innenministerium angegliedert. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er ist oberste Dienstbehörde im Sinne des § 96 der Strafprozeßordnung und trifft Enscheidungen nach §§ 64 und 65 des Landesbeamtengesetzes für das Land Nordrhein-Westfalen für sich und seine Bediensteten in eigener Verantwortung. Im übrigen untersteht er der Dienstaufsicht des Innenministers.

(4) Dem Landesbeauftragten für den Datenschutz ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Innenministers in einem eigenen Kapitel auszuweisen.

(5) In Personalangelegenheiten hat der Landesbeauftragte für den Datenschutz ein Vorschlagsrecht. Die Stellen sind im Einvernehmen mit ihm zu besetzen. Die Bediensteten können nur im Einvernehmen mit ihm versetzt oder abgeordnet werden; sie unterstehen seinen Weisungen.

(6) Der Landesbeauftragte für den Datenschutz kann sich jederzeit an den Landtag wenden.

§ 24

Berufung und Rechtsstellung

(1) Der Landtag wählt auf Vorschlag der Landesregierung einen Landesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Dieser muß die Befähigung zum Richteramt oder zum höheren Dienst haben und die zur Erfüllung seiner Aufgaben erforderliche Fachkunde besitzen.

(2) Der Landesbeauftragte für den Datenschutz ist dem Innenministerium angegliedert. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Im übrigen untersteht er der Dienstaufsicht des Innenministers.

(3) Der Landesbeauftragte für den Datenschutz wird jeweils auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen.

§ 25

Personal und Sachmittel

(1) Dem Landesbeauftragten für den Datenschutz ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Innenministers in einem eigenen Kapitel auszuweisen.

(2) In Personalangelegenheiten hat der Landesbeauftragte für den Datenschutz ein Vorschlagsrecht. Die Bediensteten unterstehen seinen Weisungen.

§ 31

Sonstige Rechte und Pflichten

(3) Der Landesbeauftragte für den Datenschutz kann sich jederzeit an den Landtag wenden.

§ 22

Aufgaben

(1) Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen, soweit sie nach diesem Gesetz seiner Kontrolle unterliegen oder sich gemäß § 11 Abs. 3 oder § 28 Abs. 4 seiner Kontrolle unterworfen haben.

(2) Der Landesbeauftragte für den Datenschutz beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, der Zuständigkeitsabgrenzung zwischen den Organen der kommunalen Selbstverwaltung sowie zwischen der staatlichen Verwaltung und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

(3) Der Landesbeauftragte für den Datenschutz kann Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere kann er die Landesregierung und einzelne Minister, die Gemeinden und Gemeindeverbände sowie die übrigen öffentlichen Stellen in Fragen des Datenschutzes beraten. Er ist über Planungen des Landes zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten, sofern in den Systemen personenbezogene Daten verarbeitet werden sollen.

(4) Auf Ersuchen des Landtags, des Petitionsausschusses des Landtags und des für den Datenschutz zuständigen Landtagsausschusses oder der Landesregierung kann der Landesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachgehen.

(5) Der Landtag und die Landesregierung können den Landesbeauftragten für den Datenschutz mit der Erstattung von Gutachten und Stellungnahmen oder der Durchführung von Untersuchungen in Datenschutzfragen betrauen. § 21 Abs. 3 Satz 2 bleibt unberührt.

(6) Der Landesbeauftragte für den Datenschutz arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach §§ 30 und 40 des Bundesdatenschutzgesetzes zusammen.

§ 26

Aufgaben

(1) Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, den Gemeinden und Gemeindeverbänden sowie den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen. Diese sind verpflichtet, den Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich gemäß § 7 Abs. 1 Satz 2 seiner Kontrolle unterworfen haben.

(2) Der Landesbeauftragte für den Datenschutz kann Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere kann er die Landesregierung und einzelne Minister, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen in Fragen des Datenschutzes beraten.

(3) Soweit es zur Erfüllung seiner Aufgaben erforderlich ist, kann der Landesbeauftragte für den Datenschutz insbesondere

1. *von den in Absatz 1 genannten Stellen Auskunft zu den Fragen sowie Einsicht in die Unterlagen und Akten verlangen, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten, die Datenverarbeitungsprogramme und die Programmunterlagen,*
2. *die in Absatz 1 genannten Stellen jederzeit unangemeldet aufsuchen und ihre Diensträume betreten.*

Der Landesbeauftragte für den Datenschutz beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und Entscheidungsbefugnisse der in § 1 Abs. 2 genannten Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, der Zuständigkeitsabgrenzung zwischen den Organen der kommunalen Selbstverwaltung sowie zwischen der staatlichen Verwaltung und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

(5) Der Landesbeauftragte für den Datenschutz arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach §§ 30, 40 des Bundesdatenschutzgesetzes zusammen.

§ 31

(2) Auf Ersuchen des Landtags, des Petitionsausschusses des Landtags und des für den Datenschutz zuständigen Landtagsausschusses oder der Landesregierung kann der Landesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachgehen.

§ 28

Erstattung von Gutachten

Der Landtag und die Landesregierung können den Landesbeauftragten für den Datenschutz mit der Erstattung von Gutachten und Stellungnahmen oder der Durchführung von Untersuchungen in Datenschutzfragen betrauen. § 24 Abs. 2 Satz 2 bleibt unberührt.

§ 23

Dateienregister

(1) Die speichernde Stelle ist verpflichtet, dem Landesbeauftragten für den Datenschutz die Beschreibung aller automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert sind, mit den Angaben der Dateibeschreibung (§ 8 Abs. 1) vorzulegen. Der Landesbeauftragte für den Datenschutz führt ein Register dieser Dateien (Dateienregister).

Der Landesbeauftragte für den Datenschutz erteilt auf Antrag unentgeltlich schriftlich Auskunft aus dem Register, soweit der Antragsteller ein berechtigtes Interesse darlegt. Das Dateienregister kann von jedermann eingesehen werden. Auskunfts- und Einsichtsrecht gelten nicht für die von den in § 18 Abs. 5 und § 2 Abs. 2 Satz 1 genannten Stellen gemeldeten Dateien.

(3) Das Nähere regelt die Landesregierung durch Rechtsverordnung, die im Einvernehmen mit dem zuständigen Landtagsausschuß ergeht.

§ 27

Register

(1) Der Landesbeauftragte für den Datenschutz führt ein Register der Dateien, in denen personenbezogene Daten gespeichert werden. Das Register kann von jedermann eingesehen werden.

(2) Das Register enthält

1. *die Angabe der Behörden und sonstigen öffentlichen Stellen, die personenbezogene Daten verarbeiten,*
2. *die Art der von ihnen oder in ihrem Auftrag gespeicherten personenbezogenen Daten,*
3. *die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,*
4. *den betroffenen Personenkreis,*
5. *die Empfänger oder Empfängergruppen, an die personenbezogene Daten übermittelt werden,*
6. *die Art der zu übermittelnden Daten sowie*
7. *die Voraussetzungen für die Übermittlung.*

Die Nummern 5 bis 7 finden keine Anwendung, wenn sich die Übermittlung auf die in § 15 Abs. 2 Nr. 1 dieses Gesetzes und die in § 12 Abs. 1 Nr. 1 Bundesdatenschutzgesetz genannten Behörden bezieht.

(3) Die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und

Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen sind verpflichtet, die von ihnen geführten Dateien im Sinne dieses Gesetzes beim Landesbeauftragten für den Datenschutz anzumelden und dabei die für die Führung des Registers erforderlichen Angaben zu machen.

(4) Die von den Behörden des Verfassungsschutzes geführten Dateien unterliegen nicht der Meldepflicht. Über die Dateien der übrigen in § 15 Abs. 2 Nr. 1 genannten Stellen wird ein gesondertes Register geführt, das sich auf Angaben über Art und Verwendung der gespeicherten Daten beschränkt. Auf dieses Register findet Absatz 1 Satz 2 keine Anwendung.

(5) Ein gesondertes Register wird für die Dateien der öffentlich-rechtlichen Unternehmen, die am Wettbewerb teilnehmen, sowie der öffentlich-rechtlichen Kreditinstitute, ihrer Zusammenschlüsse und Verbände geführt. Auf dieses Register findet Absatz 1 Satz 2 keine Anwendung.

(6) Das Nähere regelt die Landesregierung durch Rechtsverordnung, die im Einvernehmen mit dem zuständigen Landtagsausschuß ergeht.

§ 24

Beanstandungen durch den Landesbeauftragten

(1) Stellt der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes, gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er diese

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,
2. bei der Kommunalverwaltung gegenüber der jeweils verantwortlichen Gemeinde oder dem verantwortlichen Gemeindeverband,
3. bei den wissenschaftlichen Hochschulen, Gesamthochschulen und Fachhochschulen gegenüber dem Hochschulpräsidenten oder dem Rektor, bei öffentlichen Schulen gegenüber dem Leiter der Schule,
4. bei den sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nrn. 2 bis 4 unterrichtet der Landesbeauftragte für den Datenschutz gleichzeitig auch die zuständige Aufsichtsbehörde.

§ 30

Beanstandungen

(1) Stellt der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder anderer Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so teilt er diese

1. *bei der Landesverwaltung der zuständigen obersten Landesbehörde,*
2. *bei der Kommunalverwaltung der jeweils verantwortlichen Gemeinde oder dem verantwortlichen Gemeindeverband,*
3. *bei den wissenschaftlichen Hochschulen, Gesamthochschulen und Fachhochschulen dem Hochschulpräsidenten oder dem Rektor,*
4. *bei den sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts dem Vorstand oder dem sonst vertretungsberechtigten Organ*

zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist mit (Beanstandungen). In den Fällen von Satz 1 Nrn. 2 bis 4 unterrichtet der Landesbeauftragte für den Datenschutz gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Landesbeauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt oder wenn ihre Behebung sichergestellt ist.

(3) Mit der Beanstandung kann der Landesbeauftragte für den Datenschutz Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Absatz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Landesbeauftragten für den Datenschutz getroffen worden sind. Die in Absatz 1 Nrn. 2 bis 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz zu.

§ 25

Anrufungsrecht des Betroffenen

(1) Jedermann hat das Recht, sich unmittelbar an den Landesbeauftragten für den Datenschutz zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine der Kontrolle des Landesbeauftragten unterliegende Stelle in seinen Rechten verletzt zu sein; dies gilt auch für Bedienstete der öffentlichen Stellen.

(2) Niemand darf deswegen benachteiligt oder gemaßregelt werden, weil er sich an den Landesbeauftragten für den Datenschutz wendet.

§ 26

Durchführung der Kontrolle

(1) Die öffentlichen Stellen sind verpflichtet, den Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm Amtshilfe zu leisten. Ihm ist dabei insbesondere

1. Auskunft auf die Fragen zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,
2. Zutritt zu allen Diensträumen zu gewähren.

(2) Eine Beschränkung seiner Informations- und Kontrollrechte ist nur zulässig, wenn und soweit im Einzelfall ihrer Ausübung der Schutz der Sicherheit des Bundes oder eines Landes entgegensteht; diese Feststellung ist dem Ministerpräsidenten und den Ministern vorbehalten.

(2) Der Landesbeauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(3) Mit der Beanstandung kann der Landesbeauftragte für den Datenschutz Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Absatz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Landesbeauftragten für den Datenschutz getroffen worden sind. Die in Absatz 1 Nrn. 2 bis 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz zu.

§ 29

Anrufungsrecht

Jedermann hat das Recht, sich unmittelbar an den Landesbeauftragten für den Datenschutz zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine der in § 1 Abs. 2 genannten Stellen in seinen schutzwürdigen Belangen verletzt zu sein.

§ 26

Aufgaben

(1) Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, den Gemeinden und Gemeindeverbänden sowie den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen. Diese sind verpflichtet, den Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Datenschutzvorschriften auch bei den Stellen, die sich gemäß § 7 Abs. 1 Satz 2 seiner Kontrolle unterworfen haben.

(6) Die Landesregierung, die Behörden und Einrichtungen des Landes, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen haben

dem Landesbeauftragten für den Datenschutz bei der Durchführung seiner Aufgaben Amtshilfe zu leisten.

§ 27

Tätigkeitsberichte

Der Landesbeauftragte für den Datenschutz legt dem Landtag und der Landesregierung jeweils für zwei Kalenderjahre einen Bericht über seine Tätigkeit vor. Die Landesregierung legt hierzu ihre Stellungnahme dem Landtag vor; gleichzeitig gibt sie einen Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden.

§ 31

Sonstige Rechte und Pflichten

(1) Der Landesbeauftragte für den Datenschutz erstattet dem Landtag und der Landesregierung jährlich zum 31. März, erstmals 1980, einen Bericht über seine Tätigkeit. Die Landesregierung legt ihre Stellungnahme zu dem Bericht dem Landtag vor.

Dritter Teil

Besonderer Datenschutz

§ 28

Datenverarbeitung für wissenschaftliche Zwecke

(1) Öffentliche Stellen, die wissenschaftliche Forschung betreiben, dürfen personenbezogene Daten zur Durchführung eines bestimmten Forschungsvorhabens verarbeiten, soweit der Betroffene eingewilligt hat. Ohne Einwilligung des Betroffenen dürfen diejenigen Personen, die innerhalb einer öffentlichen Stelle aufgrund ihrer Zuständigkeiten Zugriff auf den jeweiligen Datenbestand haben, die vorhandenen personenbezogenen Daten zur Durchführung eines bestimmten Forschungsvorhabens verarbeiten, wenn dies im öffentlichen Interesse liegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. In anderen Fällen bedarf es der Einwilligung nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Geheimhaltungsinteresse des Betroffenen überwiegt. Behörden und Einrichtungen des Landes unterrichten in den Fällen des Satzes 3 die zuständige oberste Landesbehörde oder eine von dieser bestimmten Stelle; die übrigen öffentlichen Stellen haben in diesen Fällen den Landesbeauftragten für den Datenschutz zu unterrichten.

(2) Datenübermittlungen sind mit Einwilligung des Betroffenen zulässig, ohne Einwilligung nur nach Maßgabe des Absatzes 1 Satz 3; Absatz 1 Satz 4 gilt entsprechend. Eine anderweitige Verwendung der übermittelten Daten ist unzulässig.

(3) Die Daten sind so bald wie möglich derart zu verändern, daß ein Bezug auf eine bestimmte natürliche Person nicht mehr erkennbar ist (anonymisieren). Die Merkmale, mit deren Hilfe dieser Bezug wieder hergestellt werden kann (deanonymisieren), sind gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck dies gestattet.

§ 12

Datenverarbeitung für wissenschaftliche Zwecke

(1) Hochschulen und andere öffentliche Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung können im Rahmen ihrer Aufgaben für bestimmte Forschungsvorhaben personenbezogene Daten speichern und verändern; hierfür können ihnen die in § 1 Abs. 2 genannten Behörden und öffentlichen Stellen personenbezogene Daten übermitteln. Die Datenverarbeitung nach Satz 1 ist nur zulässig, wenn die Betroffenen eingewilligt haben, oder wenn ihre schutzwürdigen Belange nicht beeinträchtigt werden. Die übermittelnden Stellen haben die Übermittlung beim Landesbeauftragten für den Datenschutz anzuzeigen.

(2) Die nach Absatz 1 gespeicherten, veränderten und übermittelten personenbezogenen Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen diesem personenbezogene Daten nur übermittelt werden, wenn er sich verpflichtet, die Vorschriften des Absatzes 2 Satz 2 und des Absatzes 3 einzuhalten, und sich, sofern das Forschungsvorhaben im Geltungsbereich dieses Gesetzes durchgeführt werden soll, der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft. Bei einer Datenübermittlung an Stellen außerhalb des Geltungsbereichs dieses Gesetzes hat die übermittelnde Stelle die für den Empfänger zuständige Datenschutzkontrollbehörde zu unterrichten.

(5) Die wissenschaftliche Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

a) der Betroffene eingewilligt hat oder

b) dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist.

§ 29

Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Öffentliche Stellen dürfen Daten ihrer Bewerber und ihrer Beschäftigten nur verarbeiten, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. Die Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig. § 16 Abs. 1 Buchstabe c bleibt unberührt.

(2) Die Weiterverarbeitung der bei ärztlichen oder psychologischen Untersuchungen und Tests zum Zwecke des Abschlusses eines Dienst- oder Arbeitsverhältnisses erhobenen Daten ist nur mit Einwilligung des Bewerbers zulässig. Die Einstellungsbehörde darf vom untersuchenden Arzt in der Regel nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und dabei festgestellter Risikofaktoren verlangen.

(3) Personenbezogene Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, es sei denn, daß der Betroffene in die weitere Speicherung eingewilligt hat. Nach Beendigung eines Dienst- oder Arbeitsverhältnisses sind personenbezogene Daten zu löschen, wenn diese Daten nicht mehr

benötigt werden, es sei denn, daß Rechtsvorschriften entgegenstehen; § 19 Abs. 3 Satz 2 und Absatz 4 finden Anwendung.

(4) Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies auch dem Schutz des Beschäftigten dient. Beurteilungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

(5) Soweit Daten der Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

§ 30

Fernmessen und Fernwirken

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmeßdienste) in Wohnungen oder Geschäftsräumen nur vornehmen, wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen andere Wirkungen auszulösen (Fernwirkdienste). Die Einrichtung von Fernmeß- und Fernwirkdiensten ist nur zulässig, wenn der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist; dies gilt nicht für Fernmeß- und Fernwirkdienste der Versorgungsunternehmen. Der Betroffene kann seine Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Eine Leistung, der Abschluß oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, daß der Betroffene nach Absatz 1 Satz 1 oder Satz 2 einwilligt. Verweigert oder widerruft er seine Einwilligung, so dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(3) Soweit im Rahmen von Fernmeß- oder Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

§ 31

Nutzung von Verwaltungsdaten für die Erstellung von Statistiken

Für die Erstellung von Statistiken dürfen öffentliche Stellen personenbezogene Daten weiterverarbeiten, soweit diese bei der rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben angefallen sind. Die Veröffentlichungen dürfen keine Angaben enthalten, die den Bezug auf eine bestimmte Person zulassen.

§ 32

Nutzung von Einzelangaben aus der amtlichen Statistik durch Gemeinden und Gemeindeverbände

(1) Dürfen den Gemeinden und Gemeindeverbänden aufgrund gesetzlicher Ermächtigungen zur Durchführung eigener statistischer Aufgaben Einzelangaben aus der amtlichen Statistik (Datensätze) für ihren Zuständigkeitsbereich übermittelt werden, so ist dies nur zulässig auf Datenträgern, die zur maschinellen Weiterverarbeitung bestimmt sind.

(2) Datenträger dürfen nur den für die Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände übermittelt werden, die organisatorisch und räumlich von den anderen Verwaltungsstellen der Körperschaft getrennt, gegen den Zutritt unbefugter Personen hinreichend geschützt und mit eigenem Personal ausgestattet sind, das die Gewähr für Zuverlässigkeit und Verschwiegenheit bietet, schriftlich auf das Statistikgeheimnis verpflichtet worden und während der Tätigkeit in der Statistikdienststelle nicht mit anderen Aufgaben des Verwaltungsvollzuges betraut ist.

(3) Die in den Statistikdienststellen der Gemeinden und Gemeindeverbände tätigen Personen dürfen die aus den nach Absatz 1 übermittelten Einzelangaben gewonnenen personenbezogenen Erkenntnisse während und nach ihrer Tätigkeit in der Statistikdienststelle nicht in anderen Verfahren oder für andere Zwecke verarbeiten oder offenbaren.

(4) Eine Durchführung eigener statistischer Aufgaben im Sinne des Absatzes 1 liegt nur vor, wenn aus den übermittelten Einzelangaben aufgrund vorgegebener sachlicher Kriterien Zahlensummen (Tabellen) erstellt werden, aus denen kein Bezug auf eine bestimmte Person hergestellt werden kann. Die Speicherung der übermittelten Einzelangaben in Dateien für andere als statistische Nutzungen und ihre Zusammenführung mit anderen Einzelangaben, aus denen ein Bezug zu personenbezogenen Daten hergestellt werden kann, sind unzulässig.

(5) Die Übermittlung nach Absatz 1 ist nach Zeitpunkt, Art der übermittelten Daten, Zweck der Übermittlung und Empfänger von der übermittelnden Dienststelle, nach Art und Zeitpunkt der Nutzung von der Dienststelle, die die Daten erhalten hat, aufzuzeichnen. Die Aufzeichnungen sind fünf Jahre aufzubewahren.

Vierter Teil

Straf- und Bußgeldvorschriften; Übergangsvorschriften

§ 33

Straftaten

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, verändert, weitergibt oder zur Einsichtnahme bereithält,
2. abruft oder durch unrichtige Angaben erschleicht,
3. nutzt oder nicht nur für den Zweck verwendet, für den sie ihm übermittelt wurden,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen anonymisierte Daten deanonymisiert. Der Versuch ist strafbar.

(2) Absatz 1 findet nur Anwendung, soweit die Tat nicht nach anderen Vorschriften mit Strafe bedroht ist.

§ 34

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, verändert, weitergibt oder zur Einsichtnahme bereithält
2. abruft oder durch unrichtige Angaben erschleicht,
3. nutzt oder nicht nur für den Zweck verwendet, für den sie ihm übermittelt wurden.

Ordnungswidrig handelt auch, wer unter den in Satz 1 genannten Voraussetzungen anonymisierte Daten deanonymisiert.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutschen Mark geahndet werden.

Sechster Abschnitt

Straf- und Bußgeldvorschriften

§ 33

Straftaten

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. *übermittelt oder verändert oder*
2. *abruft oder sich aus in Behältnissen verschlossenen Dateien Daten verschafft,*

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, einen anderen zu schädigen oder sich oder einen anderen zu bereichern, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(3) Die Tat wird nur auf Antrag verfolgt. Der Antrag kann auch von dem Landesbeauftragten für den Datenschutz mit Zustimmung des Betroffenen gestellt werden.

§ 34

Ordnungswidrigkeit

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 13 Abs. 2 die ihm übermittelten Daten nicht nur für den Zweck verwendet, zu dessen Erfüllung sie ihm übermittelt wurden.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 Deutsche Mark geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten (OWiG) ist

1. für die Regierungsbezirke Arnsberg, Detmold und Münster der Regierungspräsident Arnsberg,
2. für die Regierungsbezirke Düsseldorf und Köln der Regierungspräsident Köln.

Siebenter Abschnitt

Übergangs- und Schlußvorschriften

§ 35

Übergangsvorschriften

(1) In Akten, die bei Inkrafttreten des Gesetzes vorhanden waren, ist die Berichtigung, Löschung oder Sperrung nur vorzunehmen, wenn die datenverarbeitende Stelle deren Voraussetzungen bei der Erfüllung ihrer laufenden Aufgaben oder aufgrund eines Überprüfungsersuchens des Betroffenen feststellt.

(2) Für Behörden des Justizvollzuges gilt § 18 mit der Maßgabe, daß der Betroffene Auskunft oder Akteneinsicht erhält, soweit er zur Wahrnehmung seiner Rechte oder berechtigten Interessen auf die Kenntnis gespeicherter Daten angewiesen ist.

§ 35

Übergangsvorschrift

(1) Die Veröffentlichung über personenbezogene Daten (§ 15), die beim Inkrafttreten des Gesetzes schon gespeichert waren, hat binnen eines Jahres nach Inkrafttreten des Gesetzes zu erfolgen.

(2) Sind im Anwendungsbereich der §§ 18 bis 23 dieses Gesetzes personenbezogene Daten bereits vor dem Inkrafttreten dieses Gesetzes gespeichert worden, so ist der Betroffene darüber nach § 22 Abs. 1 zu benachrichtigen, wenn die Daten erstmals nach dem Inkrafttreten des Gesetzes übermittelt werden.

Artikel 2

Datenschutzveröffentlichungsverordnung Nordrhein-Westfalen

Die Verordnung über die Veröffentlichung der Angaben über gespeicherte personenbezogene Daten (Datenschutzveröffentlichungsverordnung – DSVeröffVO NW –) vom 6. November 1979 (GV. NW. S. 726) wird aufgehoben.

Artikel 3

Änderung des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen

Verwaltungsverfahrensgesetz für das Land Nordrhein-Westfalen (VwVfG. NW.)

Das Verwaltungsverfahrensgesetz für das Land Nordrhein-Westfalen (VwVfG. NW) vom 21. Dezember 1976 (GV. NW. S. 438), geändert durch Gesetz vom 6. November 1984 (GV. NW. S. 663), wird wie folgt geändert:

1. Nach § 3 wird folgender neuer § 3a eingefügt:

   „§ 3a

   Personenbezogene Daten, Betriebs- und Geschäftsgeheimnisse

   Die Behörde darf Angaben über persönliche und sachliche Verhältnise einer natürlichen Person sowie Betriebs- oder Geschäftsge-

heimnisse nicht unbefugt offenbaren. Sie unterliegt, soweit sie personenbezogene Daten verarbeitet, den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen."

2. § 26 wird wie folgt geändert:

   a) In Absatz 1 Satz 1 werden nach dem Wort „sich" die Worte „unter Beachtung des § 3a" eingefügt.

   b) In Absatz 2 Satz 3 werden nach dem Wort „Erscheinen" ein Komma und die Wörter „zur Angabe von personenbezogenen Daten oder von Betriebs- und Geschäftsgeheimnissen" eingefügt. Nach Absatz 2 Satz 3 wird folgender Satz 4 angefügt:

   „Der Auskunftspflichtige kann die Auskunft auf solche Fragen, zu deren Beantwortung er durch Rechtsvorschrift verpflichtet ist, verweigern, wenn deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nrn. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde."

3. § 30 wird aufgehoben.

§ 26

Beweismittel

(1) Die Behörde bedient sich der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Sie kann insbesondere

1. Auskünfte jeder Art einholen,

2. Beteiligte anhören, Zeugen und Sachverständige vernehmen oder die schriftliche Äußerung von Beteiligten, Sachverständigen und Zeugen einholen,

3. Urkunden und Akten beiziehen,

4. den Augenschein einnehmen.

(2) Die Beteiligten sollen bei der Ermittlung des Sachverhalts mitwirken. Sie sollen insbesondere ihnen bekannte Tatsachen und Beweismittel angeben. Eine weitergehende Pflicht, bei der Ermittlung des Sachverhalts mitzuwirken, insbesondere eine Pflicht zum persönlichen Erscheinen oder zur Aussage, besteht nur, soweit sie durch Rechtsvorschrift besonders vorgesehen ist.

(3) Für Zeugen und Sachverständige besteht eine Pflicht zur Aussage oder zur Erstattung von Gutachten, wenn sie durch Rechtsvorschrift vorgesehen ist. Falls die Behörde Zeugen und Sachverständige herangezogen hat, werden sie auf Antrag in entsprechender Anwendung des Gesetzes über die Entschädigung von Zeugen und Sachverständigen entschädigt.

§ 30

Geheimhaltung

Die Beteiligten haben Anspruch darauf, daß ihre Geheimnisse, insbesondere die zum persönlichen Lebensbereich gehörenden Geheimnisse sowie die Betriebs- und Geschäftsgeheimnisse, von der Behörde nicht unbefugt offenbart werden.

Artikel 4

Änderung des Meldegesetzes für das Land Nordrhein-Westfalen

Das Meldegesetz für das Land Nordrhein-Westfalen (Meldegesetz NW – MG NW) vom 13. Juli 1982 (GV. NW. S. 474), geändert durch Gesetz vom 6. November 1984 (GV. NW. S. 663), wird wie folgt geändert:

1. § 3 Abs. 2 wird wie folgt geändert:

   a) Nummer 4 erhält folgende Fassung:

Meldegesetz für das Land Nordrhein-Westfalen (Meldegesetz NW – MG NW)

„4. für die Mitwirkung bei der Wehrüberwachung
die Tatsache, daß der Betroffene nach Vollendung des 32. Lebensjahres der Wehrüberwachung unterliegt,"

b) Nummer 7 erhält folgende Fassung:

„7. für die Mitwirkung bei der Erfüllung der Aufgaben nach der Dritten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens vom 30. März 1935 (RGS. NW. S. 7),
die Berufsausübung im Gesundheitswesen,"

c) Nummer 8 entfällt.

d) Nummer 9 wird Nummer 8.

e) Nummer 10 wird Nummer 9.

f) Nummer 11 wird Nummer 10.

(2) Über die in Absatz 1 genannten Daten hinaus speichern die Meldebehörden im Melderegister oder an anderer Stelle folgende Daten einschließlich der zum Nachweis ihrer Richtigkeit erforderlichen Hinweise:

1. *für die Vorbereitung von Parlaments- und Kommunalwahlen sowie von Volksbegehren und Volksentscheiden die Tatsache, daß der Betroffene vom Wahlrecht ausgeschlossen oder nicht wählbar ist,*
2. *für die Ausstellung von Lohnsteuerkarten
steuerrechtliche Daten (Steuerklasse, Freibeträge, Religionszugehörigkeit des Ehegatten, Rechtsstellung und Zuordnung der Kinder, Vor- und Familiennamen sowie Anschrift der Pflege- und Stiefeltern),*
3. *für die Ausstellung von Personalausweisen und Pässen
die Tatsache, daß Paßversagungsgründe vorliegen, ein Paß versagt oder entzogen oder eine Anordnung nach § 2 Abs. 2 des Gesetzes über Personalausweise vom 19. Dezember 1950 (BGBl. I S. 807), zuletzt geändert durch Gesetz vom 6. März 1980 (BGBl. I. S. 270), getroffen worden ist,*
4. *für die Mitwirkung bei der Wehr- oder Zivildienstüberwachung
die Tatsache, daß der Betroffene der Wehr- oder Zivildienstüberwachung unterliegt,*
5. *für die Vornahme von Ehrungen durch öffentliche Stellen sowie für die Mitwirkung bei der Erfüllung der Aufgaben nach dem Personenstandsgesetz
den Tag und den Ort der Eheschließung, soweit sie sich nicht aus den nach Absatz 1 Nr. 14 gespeicherten Daten ergeben, oder die Tatsache, daß ein Familienbuch auf Antrag angelegt worden ist,*
6. *zur Beantwortung von Aufenthaltsanfragen anderer Behörden und sonstiger öffentlicher Stellen, wenn der Einwohner die Wohnung aufgegeben hat und der Meldebehörde eine neue Wohnung nicht bekannt ist, für die Dauer von zwei Jahren
die Tatsache der Aufenthaltsanfrage (Datum der Anfrage, anfragende Stelle),*
7. *für die Feststellung der Identität des Einwohners den Beruf,*
8. *für die Feststellung der Identität des Einwohners im Rahmen von Maßnahmen der Gefahrenabwehr oder Strafverfolgung
die Seriennummer des Personalausweises und des Passes,*
9. *für die Mitwirkung bei der Erfüllung von Aufgaben nach dem Wohnungsbindungsgesetz*

(WoBindG) und dem Gesetz über den Abbau der Fehlsubventionierung im Wohnungsbau (AFWoG)
die Tatsache, daß der Einwohner in einer öffentlich geförderten Wohnung wohnt,

10. für die Mitwirkung bei der Erfüllung von Aufgaben nach dem Jugendarbeitsschutzgesetz (JArbSchG)
die Tatsache, daß für den Einwohner ein Untersuchungsberechtigungsschein ausgestellt worden ist,

11. für die Geltendmachung von Rentenansprüchen als Nachweis für den Einwohner
Daten über Zeiten im Reichsarbeitsdienst, der Wehrmacht oder in Kriegsgefangenschaft, soweit diese Daten bei der Meldebehörde vor Inkrafttreten dieses Gesetzes gespeichert gewesen sind.

(3) Als Hinweis zum Nachweis der Richtigkeit gespeicherter Daten darf nur der Verweis auf das Beweismittel, nicht aber der Inhalt des Beweismittels gespeichert werden.

§ 11

Löschung und Aufbewahrung von Daten

(1) Die Meldebehörde hat gespeicherte Daten zu löschen, wenn sie zur Erfüllung der der Meldebehörde obliegenden Aufgaben nicht mehr erforderlich sind. Das gleiche gilt, wenn ihre Speicherung unzulässig war.

2. In § 11 Abs. 2 Satz 2 werden die Wörter „nach § 3 Abs. 2 Nr. 1, 8 und 11" durch die Wörter „nach § 3 Abs. 2 Nr. 1 und 10" ersetzt.

(2) Daten eines weggezogenen oder verstorbenen Einwohners sind unverzüglich nach dem Wegzug und der Auswertung der Rückmeldung oder dem Tod des Einwohners zu löschen, die Daten nach § 3 Abs. 1 Nr. 11 und Abs. 2 Nr. 2 jedoch erst nach Ablauf des auf den Tod oder den Wegzug folgenden Kalenderjahres. Abweichend davon hat die Meldebehörde nach dem Wegzug oder dem Tod eines Einwohners weiterhin die übrigen Daten nach § 3 Abs. 1 mit Ausnahme der Daten nach § 3 Abs. 1 Nr. 8 sowie die Daten nach § 3 Abs. 2 Nr. 1, 8 und 11 zu speichern. Das gleiche gilt für die zum Nachweis der Richtigkeit dieser Daten erforderlichen Hinweise.

3. In § 11 Abs. 3 Satz 2 werden hinter den Wörtern „dürfen sie" die Wörter „mit Ausnahme der Anschrift sowie des Sterbetages und -orts" eingefügt.

(3) Nach Ablauf von fünf Jahren nach Ende des Kalenderjahres, in dem ein Einwohner weggezogen oder verstorben ist, sind die nach Absatz 2 Satz 2 und 3 gespeicherten Daten und Hinweise für die Dauer von 45 Jahren gesondert aufzubewahren und durch technische und organisatorische Maßnahmen besonders zu sichern. Während dieser Zeit dürfen sie nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zur rechtmäßigen Aufgabenerfüllung der in § 31 Abs. 3 genannten Behörden oder für Wahlzwecke

unerläßlich ist oder der Betroffene schriftlich eingewilligt hat. Nach Ablauf von 50 Jahren sind die Daten zu löschen.

(4) Der Innenminister bestimmt durch Rechtsverordnung das Nähere über das Verfahren der Löschung, der gesonderten Aufbewahrung und die erforderlichen Sicherungsmaßnahmen nach Absatz 3.

(5) Ist eine Löschung im Falle des Absatzes 1 Satz 1 wegen der besonderen Art der Speicherung im Melderegister nicht oder nur mit unverhältnismäßig hohem Aufwand möglich, ist durch technische oder organisatorische Maßnahmen sicherzustellen, daß die Daten nicht mehr verarbeitet oder sonst genutzt werden.

4. In § 18 Abs. 1 Satz 1 wird hinter den Wörtern "§ 3 Abs. 2 Nr. 2, 4, 5" das Komma durch das Wort „und" ersetzt; die Wörter „und 8" werden gestrichen.

§ 18

Datenerhebung; Meldeschein

(1) Bei der An- oder Abmeldung dürfen vom Meldepflichtigen die in § 3 Abs. 1 Nr. 1 bis 18 sowie die in § 3 Abs. 2 Nr. 2, 4, 5, 7 und 8 aufgeführten Daten erhoben werden. Für Zwecke des Suchdienstes ist von den Einwohnern, die aus den in § 1 Abs. 2 Nr. 3 des Bundesvertriebenengesetzes bezeichneten Gebieten stammen, die Anschrift vom 1. September 1939 zu erheben.

(2) Die amtliche Meldebestätigung darf folgende Daten enthalten:

Familienname,
Vornamen,
akademische Grade,
Ordensnamen, Künstlernamen,
Tag des Ein- oder Auszugs,
Anschrift.

(3) Der Innenminister bestimmt durch Rechtsverordnung die Muster der Meldescheine für die Meldungen nach § 13 Abs. 1 und 2, die Anzahl der Ausfertigungen, die Aufbewahrungsdauer bei der Meldebehörde sowie die Muster der Meldebestätigungen.

5. In § 30 Abs. 1 Satz 2 wird hinter den Wörtern „§ 3 Abs. 2 Nr. 1" das Komma durch das Wort „und" ersetzt; die Wörter „und 4" werden gestrichen.

§ 30

Datenübermittlung zwischen den Meldebehörden

(1) Hat sich ein Einwohner bei einer Meldebehörde angemeldet, so hat diese die bisher zuständige Meldebehörde und die für weitere Wohnungen zuständigen Meldebehörden davon durch Übermittlung von

1. *Vor- und Familiennamen,*
2. *Anschriften,*
3. *Tag und Ort der Geburt,*
4. *Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft,*
5. *Staatsangehörigkeit,*
6. *Tag des Zuzugs,*

7. Haupt- und Nebenwohnung sowie

8. Familienstand

des Einwohners zu unterrichten (Rückmeldung). Die bisher zuständige Meldebehörde hat die Meldebehörde der neuen Wohnung über die in § 3 Abs. 2 Nr. 1, 3 und 4 genannten Tatsachen sowie dann zu unterrichten, wenn die in Satz 1 genannten Daten von den bisherigen Angaben abweichen.

6. § 31 wird wie folgt geändert:

§ 31

Datenübermittlung an andere Behörden oder sonstige öffentliche Stellen; Datenweitergabe

a) In Absatz 1 Satz 2 werden hinter den Wörtern „§ 3 Abs. 1 Nr. 17" die Wörter „und Abs. 2 Nr. 7 und 8" gestrichen.

(1) Die Meldebehörde darf einer anderen Behörde oder sonstigen öffentlichen Stelle im Geltungsbereich des Melderechtsrahmengesetzes aus dem Melderegister

1. Vor- und Familiennamen,

2. frühere Namen,

3. akademische Grade,

4. Ordensnamen, Künstlernamen,

5. Anschriften,

6. Tag des Ein- und Auszugs,

7. Tag und Ort der Geburt,

8. Geschlecht,

9. gesetzliche Vertreter,

10. Staatsangehörigkeit,

11. Familienstand,

12. Übermittlungssperrren sowie

13. Sterbetag und -ort

übermitteln, wenn dies zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit oder der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Den in Absatz 3 bezeichneten Behörden darf die Meldebehörde unter den Voraussetzungen des Satzes 1 über die dort genannten Daten hinaus auch die Angaben nach § 3 Abs. 1 Nr. 17 und Abs. 2 Nr. 7 und 8 übermitteln. Werden diese Daten für eine Personengruppe listenmäßig oder in sonst zusammengefaßter Form übermittelt, so dürfen für die Zusammensetzung der Personengruppe nur die in Satz 1 genannten Daten zugrunde gelegt werden.

b) In Absatz 5 Satz 1 werden hinter den Wörtern „Absätze 1 und 2" die Wörter „sowie der in § 3 Abs. 2 Nr. 7" eingefügt.

(5) Der Innenminister wird ermächtigt, durch Rechtsverordnung die regelmäßige Übermittlung der in den Absätzen 1 und 2 genannten Daten zuzulassen, soweit die dort genannten Voraussetzungen erfüllt sind. Er hat hierbei Anlaß und Zweck der Übermittlung, die Datenempfänger, die zu übermittelnden Daten, ihre Form sowie das Nähere über das Verfahren der Übermittlung festzulegen.

7. § 34 Abs. 3 Satz 2 wird wie folgt geändert:

   a) In Nummer 7 wird hinter den Wörtern „oder nicht" das Komma durch einen Punkt ersetzt; das Wort „sowie" wird gestrichen.

   b) Nummer 8 wird gestrichen.

(3) Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) darf nur erteilt werden, soweit sie im öffentlichen Interesse liegt. Für die Zusammensetzung der Personengruppe dürfen die folgenden Daten herangezogen werden:

1. *Vor- und Familiennamen,*
2. *Tag der Geburt,*
3. *Geschlecht,*
4. *Staatsangehörigkeit,*
5. *Anschriften,*
6. *Tag des Ein- und Auszugs,*
7. *Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht, sowie*
8. *Beruf.*

Mitgeteilt werden dürfen folgende Daten:

1. *Vor- und Familiennamen,*
2. *akademische Grade,*
3. *Alter,*
4. *Geschlecht,*
5. *Staatsangehörigkeit,*
6. *Anschriften und*
7. *gesetzlicher Vertreter.*

8. § 35 Abs. 4 erhält folgende Fassung:

   „(4) Adreßbuchverlagen darf Auskunft über

   1. Vor- und Familiennamen,
   2. akademische Grade und
   3. Anschriften

   sämtlicher Einwohner, die das 18. Lebensjahr vollendet und dieser Auskunft nicht widersprochen haben, erteilt werden. Auf das Widerspruchsrecht ist bei der Anmeldung sowie spätestens einen Monat vor Weitergabe der Daten an den Adreßbuchverlag durch öffentliche Bekanntmachung der Meldebehörde hinzuweisen. § 34 Abs. 5 gilt entsprechend."

(4) Adreßbuchverlagen darf Auskunft über

1. *Vor- und Familiennamen,*
2. *akademische Grade und*
3. *Anschriften sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, erteilt werden. § 34 Abs. 5 gilt entsprechend.*

9. § 40 wird aufgehoben.

§ 40

Mehrere Wohnungen

Bewohnt ein Einwohner im Zeitpunkt des Inkrafttretens dieses Gesetzes mehrere Wohnungen, so hat die Meldebehörde die Hauptwohnung im Sinne des § 16 Abs. 2 auf der Grundlage der Erhebungen der nächsten Volkszählung zu bestimmen.

10. § 41 wird aufgehoben.

§ 41

Meldescheine

Bei der An- oder Abmeldung gemäß § 13 Abs. 1 und 2 dürfen Meldescheine nach dem Muster der Anlagen 1 und 2 der Verordnung zur Durchführung es Meldegesetzes für das Land Nordrhein-Westfalen (MG NW) – DVO MG NW – vom 2. Juni 1960 (GV. NW. S. 175), zuletzt geändert durch Verordnung vom 1. April 1980 (GV. NW. S. 476), bis zum 30. Juni 1983 verwendet werden mit der Maßgabe, daß die Unterschrift des Wohnungsgebers von der Meldebehörde nicht verlangt werden kann.

Artikel 5

Änderung des Gesetzes über den „Westdeutschen Rundfunk Köln"

§ 52 Abs. 1 Satz 1 des Gesetzes über den „Westdeutschen Rundfunk Köln" – WDR-Gesetz – vom 19. März 1985 (GV. NW. S. 237) erhält folgende Fassung:

„Der Rundfunkrat bestellt einen Beauftragten für den Datenschutz des WDR, der an die Stelle des Landesbeauftragten für den Datenschutz tritt."

Gesetz über den „Westdeutschen Rundfunk Köln"
– WDR-Gesetz –

§ 52

Beauftragter für den Datenschutz des WDR

(1) Der Rundfunkrat bestellt einen Beauftragten für den Datenschutz des WDR. Dieser ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Im übrigen untersteht er der Dienstaufsicht des Verwaltungsrates.

Artikel 6

Neubekanntmachungsvorschrift

Die zuständigen Minister werden ermächtigt, die durch dieses Gesetz geänderten Gesetze in der neuen Fassung mit neuem Datum und in fortlaufender Paragraphenfolge bekanntzumachen und dabei Unstimmigkeiten des Wortlauts zu berichtigen.

Artikel 7

Inkrafttreten

Dieses Gesetz tritt am Tage nach seiner Verkündung in Kraft. Zum selben Zeitpunkt werden das Datenschutzgesetz Nordrhein-Westfalen (DSG NW, vom 19. Dezember 1978 (GV. NW. S. 640), geändert durch Gesetz vom 13. Juli 1982 (GV. NW. S. 474), mit Ausnahme der §§ 38 und 39, und die Verordnung über die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Datenschutzgesetz Nordrhein-Westfalen vom 25. November 1980 (GV. NW. S. 1049) aufgehoben. Die Änderungen zu Artikel 4 Nr. 1 Buchstaben c bis f sowie zu Nr. 2, Nr. 4 und Nr. 6 Buchstabe a, soweit sich dieser auf § 3 Abs. 2 Nr. 8 bezieht, treten am 1. September 1991 in Kraft.

Begründung

Zu Artikel 1

Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nordrhein-Westfalen)

A Allgemeines

1. Ausgangslage

   a) Der Gesetzentwurf verfolgt in erster Linie das Ziel, das für die Landes- und Kommunalverwaltung in Nordrhein-Westfalen geltende allgemeine **Datenschutzgesetz** (Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung – Datenschutzgesetz Nordrhein-Westfalen – DSG NW – vom 19. 12. 1978, GV. NW. S. 640, geändert durch Gesetz vom 13. 7. 1982, GV. NW. 2. 474) im Interesse der Sicherung des informationellen Selbstbestimmungsrechts auszubauen und gleichzeitig so zu gestalten, daß es künftigen Entwicklungen der Datenverarbeitungstechnik so weit wie möglich gerecht wird (Artikel 1 und 2). Durch gleichzeitige Änderungen des **Verwaltungsverfahrensgesetzes** soll erreicht werden, daß die Bestimmungen des Datenschutzgesetzes bei jeglichem Umgang öffentlicher Verwaltungen mit personenbezogenen Daten zu beachten sind (Artikel 3). Darüber hinaus sollen im Sinne einer Verbesserung des Datenschutzes wichtige Einzelvorschriften des **Meldegesetzes** geändert werden (Artikel 4) und eine Klarstellung im Rahmen des Gesetzes über den „Westdeutschen Rundfunk Köln" erfolgen (Artikel 5). Der Entwurf greift damit – prinzipiell unverändert – die datenschutzpolitischen Vorstellungen auf, die dem bereits in der vergangenen Legislaturperiode eingebrachten, aber nicht mehr verabschiedeten **Gesetzentwurf der Landesregierung zur Fortentwicklung des Datenschutzes** vom 14. 2. 1985 (LT-Drs. 9/4075) zugrunde gelegen haben. Der frühere Entwurf hat die Überlegungen von Bund und Ländern zur Verbesserung des Datenschutzes erheblich beeinflußt; seine grundsätzlichen Aussagen sind nicht in Frage gestellt.

   Nicht allein die Zunahme der Informationsverarbeitung im öffentlichen Bereich sowie das Aufkommen veränderter Informationstechniken machen es erforderlich, Regelungen vorzusehen, die auch der potentiellen Gefahr einer zunehmenden Durchleuchtung und Vereinnahmung des einzelnen durch Staat und andere öffentliche Stellen vorbeugen und die Rechtsposition des Betroffenen wirksam verstärken. Der Ausbau des Schutzes der Persönlichkeitsrechte ist eine der wesentlichen Aufgaben eines demokratischen Rechtsstaates.

   b) Der Gesetzentwurf zieht mit einer Vielzahl neuer oder erweiterter Regelungen in einem bedeutenden Schritt die notwendigen **Konsequenzen aus dem Urteil des Bundesverfassungsgerichts** (BVerfGE 65, 1) vom 15. 12. 1983 zum Volkszählungsgesetz. Nach den grundlegenden verfassungsrechtlichen Aussagen des Gerichts wird insbesondere unter den Bedingungen der modernen Datenverarbeitung der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikels 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG umfaßt. Dieses Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (Recht auf informationelle Selbstbestimmung). Damit ist der Datenschutz als Konkretisierung eines wesentlichen Aspekts des Persönlichkeitsrechts anerkannt; er hat Verfassungsrang erhalten. Dies verpflichtet den Gesetzgeber in Bund und Ländern, das geltende Recht anhand der vom Bundesverfassungsgericht dargelegten Kriterien zu überprüfen, zu ändern oder ggfs. überhaupt erst entsprechende gesetzliche Regelungen zu schaffen. Soweit das Gericht grundsätzliche Ausführungen zur Tragweite des Rechts auf informationelle Selbstbestimmung gemacht hat, etwa zur Erhebung und zur Zweckbindung personenbezogener Daten sowie zur Erweiterung der Auskunfts- und Aufklärungspflichten, sind hieraus zwingend gesetzgeberische Konsequenzen zu ziehen. Darüber hinaus will die Landesregierung mit diesem Entwurf die vom Bundesverfassungsgericht dem Gesetzgeber überlassenen Gestaltungsmöglichkeiten aufgreifen; sie wertet die Ausführungen des Gerichts als eine politische Verpflichtung und als eine Ermunterung, auch neue Lösungsvorschläge zur Fortentwicklung des Datenschutzes zu unterbreiten.

   c) Die Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 hat zugleich die Intentionen des **Artikels 4 Absatz 2 der Landesverfassung (Recht auf Datenschutz)** bestätigt und aktualisiert. Durch diese Verfassungsvorschrift von 1978 ist erstmals in der Verfassungsrechtsgeschichte der Schutz personenbezogener Daten als ausdrücklich formuliertes Grundrecht in einer

deutschen Verfassung verankert worden. Diesem Abwehrrecht kommt – über den bisher vom Datenschutzgesetz NW geschützten Bereich der Verarbeitung personenbezogener Daten in Dateien hinaus – generelle Bedeutung für den Individualrechtsschutz im Rahmen der Informationsverarbeitung zu. Grundsätzlich ist hiernach für jeden behördlichen Umgang mit personenbezogenen Daten eine materiell-gesetzliche Grundlage erforderlich (vgl. auch OVG Münster, Beschluß vom 4. 4. 1979, OVGE Bd. 34 Seite 103ff.). Mit der Neufassung des Datenschutzgesetzes soll deshalb auch ein allgemeines Ausführungsgesetz zu dieser Verfassungsnorm geschaffen werden. Die Notwendigkeit besonderer ergänzender oder abweichender Regelungen für bestimmte Bereiche (bereichsspezifische Regelungen) wird damit nicht in Frage gestellt.

d) Bei der vorgesehenen Novellierung der datenschutzrechtlichen Vorschriften sollen auch die **Erfahrungen aus der Praxis** bei der Anwendung der allgemeinen Datenschutzgesetze Berücksichtigung finden. Einen beachtlichen Beitrag zur Fortentwicklung des Datenschutzes in Nordrhein-Westfalen hat der Landesbeauftragte für den Datenschutz Nordrhein-Westfalen geleistet. Erkenntnisse der Aufsichtsbehörden sind in den Gesetzentwurf eingeflossen. Wichtige Anstöße zur Novellierung des Datenschutzgesetzes sind in der Vergangenheit auch von den Fraktionen des Landtages ausgegangen. Ein wachsendes Bewußtsein für die Notwendigkeit einer Verbesserung des Schutzes personenbezogener Daten spiegelt auch der Stand der öffentlichen Diskussion wider: Das Anliegen des Datenschutzes hat beträchtliche Resonanz in der interessierten Öffentlichkeit gefunden und zu einem „öffentlichen Datenschutzbewußtsein" geführt. Die notwendige Akzeptanz der Datenverarbeitung durch den Bürger wird deshalb wesentlich mitbestimmt durch die Qualität der Datenschutzregelungen.

e) Datenschutzregelungen müssen auch **neueren Entwicklungen in der Informationstechnik** und den aus ihnen folgenden organisatorischen Veränderungen so weit wie möglich Rechnung tragen. Gegenüber den Verhältnissen zum Ende der 70er Jahre hat sich die Situation in der Informationstechnik erheblich gewandelt*). Neue Einsatzmöglichkeiten der automatisierten Datenverarbeitung zeichnen sich danach in der öffentlichen Verwaltung ab. Auf der Basis der von der Bundespost angebotenen neuen Kommunikationsdienste wird die öffentliche Verwaltung ihre Aufgaben rationeller als bisher betreiben und ihre Informationssysteme untereinander vernetzen können. Datenverarbeitung und Nachrichtentechnik werden zu einer unlösbaren Gesamtheit und verändern die Arbeitsabläufe im Dienstleistungssektor. Durch den Rückgang der Hardwarekosten wird ein dezentraler Einsatz von Datenverarbeitungsgeräten wirtschaftlich eher möglich. Mit zunehmender Leistungsfähigkeit der Kleinrechner und der Netzwerke werden Funktionen der Verarbeitungsprozesse bis hin zur Erledigung einfacher oder spezieller Aufgaben aus den bisherigen Rechenzentren auf ein Datenverarbeitungsgerät am Arbeitsplatz zurückgeführt werden können. Die bisherige strikte Trennung zwischen automatisierter Datenverarbeitung und traditioneller Bürotechnik wird durch die zunehmende Integration der Mikroelektronik in Bürogeräten auf mittlere Sicht überwunden. Dies ist auch einer der Gründe, die konventionellen Formen der Datenverarbeitung auch außerhalb der Dateien in den Anwendungsbereich des Gesetzes einzubeziehen. Die modifizierten technischen Basisstrukturen, die bereits zu einer Überprüfung der bisher an den großen Rechenzentren orientierten Organisationsregelungen Veranlassung gegebenen haben (Gesetz zur Änderung des Gesetzes über die Organisation der automatisierten Datenverarbeitung in Nordrhein-Westfalen – ADVG NW – vom 20. 12. 1984 – GV. NW. S. 750 –), berühren zumindest potentiell in höherem Maße das Recht des Bürgers auf Wahrung seines Persönlichkeitsbereichs als bisher. Solche technischen Gefährdungspotentiale müssen im Interesse des Bürgers begrenzt und auch sozialverträglich eingebunden werden.

f) Gleichwohl ist das **Verhältnis veränderter Informationstechnik zu den gesetzgeberischen Möglichkeiten** nicht ohne Probleme: Die technische Entwicklung kann nur für einen begrenzten Zeitraum übersehen werden. Der Entwurf versteht sich insoweit als **ein** weiterer Schritt zur Verbesserung des Datenschutzes. Die Datenschutzgesetzgebung kann keine Antworten auf Probleme geben, die – jedenfalls im gegenwärtigen Zeitpunkt – noch nicht näher definiert werden können. Das vorgesehene Regelungsmodell für den Datenschutz geht nach wie vor von einer prinzipiellen Überschaubarkeit der Informationsströme aus. Seit der Einführung des Bildschirmtextes wird zwar die Frage nach den Grenzen eines solchen Modells aufgeworfen. Aber selbst in den von manchen erwarteten prinzipiell offenen Kommunikationssystemen werden die zentralen Begriffe des Datenschutzes ihre Bedeutung nicht verlieren. Dies gilt insbesondere für die Schutzrechte des

*) *vgl. auch Bericht des Innenministers vom Oktober 1986 „Einsatz der Informationstechnik in der Landesverwaltung Nordrhein-Westfalen – Bilanz und Perspektiven"*

Betroffenen. Die beispielsweise im Bildschirmtextstaatsvertrag erzielten Datenschutzregelungen belegen zudem, daß neuauftretende Probleme zumindest im Rahmen der bereichsspezifischen Datenschutzgesetzung aufgearbeitet und gelöst werden können. Bisher liegen auch keine konkreten Lösungsvorschläge für eine ganz neue Datenschutzkonzeption vor. Der Gesetzgeber kann sich aber nicht an futuristischen Aspekten der Informations- und Kommunikationstechnik orientieren. Auf solche Probleme Antworten zu finden, bleibt einem späteren Zeitpunkt überlassen. Abgesehen davon, daß daher eine Alternative zur Grundkonzeption des Datenschutzgesetzes nicht ersichtlich ist, hält die Landesregierung die vorgesehene Neufassung dieses Gesetzes zur Anpassung an die technische Entwicklung auf dem Gebiet der Informationsverarbeitung derzeit für ausreichend.

2. Datenschutzpolitische Grundlinien des Entwurfs

a) **Fortentwicklung des Datenschutzes** in Nordrhein-Westfalen bedeutet in erster Linie **Novellierung des allgemeinen Datenschutzgesetzes.** Als weitgespannte **Rahmenregelung** und wegen seiner **Leitfunktion** für andere landesrechtliche Datenschutzregelungen kommt dem allgemeinen Datenschutzgesetz besondere Bedeutung zu. In dieser Funktion muß das Datenschutzgesetz generelle Anforderungen an den Umgang mit personenbezogenen Daten in der öffentlichen Verwaltung stellen.

Nur wenn aus Gründen des Gemeinwohls Eingriffe in das informationelle Selbstbestimmungsrecht unter anderen – insbesondere erleichterten – Voraussetzungen zugelassen werden sollen, so bedarf es hierzu einer bereichsspezifischen Entscheidung des Gesetzgebers. Die Datenschutzgesetzgebung hat in den letzten Jahren zunehmend Lösungen im Rahmen bereichsspezifischer Regelungen gesucht. Für den Bereich des Landes Nordrhein-Westfalen sind hier beispielsweise zu nennen: das Verfassungsschutzgesetz, das Meldegesetz, der Bildschirmtext-Staatsvertrag, das Kabelversuchsgesetz und das Krebsregistergesetz. Solche datenschutzrechtlichen Sonderregelungen werden auch in Zukunft unverzichtbar sein. Dennoch kann sich die Fortentwicklung des Datenschutzes nicht ausschließlich in bereichsspezifisch angelegten Datenschutznormen vollziehen. Ist es schon gesetzgebungstechnisch unmöglich, für alle Lebenssachverhalte derartige Regelungen zu treffen, so sprechen vor allem gewichtige rechtspolitische Gesichtspunkte dagegen, den – bis zu einem gewissen Grade unvermeidlichen – Verrechtlichungsprozeß in solcher Weise voranzutreiben, daß nahezu jedes Informationsverhalten im öffentlichen Bereich spezialgesetzlich geregelt wäre. Eine solche Verfahrensweise würde nicht nur zu einer unvertretbaren Normenflut führen, sondern auch die Leitfunktionen des allgemeinen Datenschutzgesetzes ohne Not in Frage stellen. Wesentliches Ziel dieser Novelle ist es deshalb, soweit wie nur möglich bereichsspezifische Sonderregelungen entbehrlich zu machen. Dieses Ziel kann aber nur erreicht werden, wenn das Datenschutzgesetz eine wirklich angemessene Antwort auf die Probleme des Datenschutzes gibt.

Mit diesem Gesetzentwurf unternimmt die Landesregierung daher den Versuch, für viele Lebenssachverhalte die angemessene Lösung aus dem Spannungsverhältnis zwischen dem Persönlichkeitsrecht des einzelnen und dem Gemeinwohl sowie etwa entgegenstehenden Rechten Dritter zu entwickeln. Mit seiner umfassend angelegten Datenschutzkonzeption für den Umgang mit personenbezogenen Daten in der öffentlichen Verwaltung betritt der Entwurf zwangsläufig in manchen Datenschutzfragen Neuland. Die vorgelegten Lösungsvorschläge beruhen jedoch auf einer sorgfältigen Ermittlung der konkurrierenden Interessen und berücksichtigen auch die Belange der Verwaltungspraxis, soweit dies gegenüber dem informationellen Selbstbestimmungsrecht zulässig ist.

b) Prinzipiell wird **jeder Umgang** der öffentlichen Verwaltung **mit personenbezogenen Daten ohne Rücksicht auf die jeweilige Form der Verarbeitung als Eingriff** in das informationelle Selbstbestimmungsrecht **gewertet.** Dies führt zu einer grundsätzlichen Einbeziehung auch der traditionellen Formen der Informationsverarbeitung (Akten) in den Schutzbereich des Datenschutzgesetzes und zwingt zu einer Abkehr von der am Anfang der Datenschutzdiskussion stehenden Vorstellung, nur den Mißbrauch bei der automatisierten oder dateimäßigen Verarbeitung personenbezogener Daten zu verhindern. Die Verarbeitung personenbezogener Daten in und aus Akten kann auch im Einzelfall einen sehr viel stärkeren Eingriff darstellen als die Verarbeitung dateimäßig gespeicherter personenbezogener Daten. In verschiedenen bereichsspezifischen Datenschutzregelungen des Bundes und der Länder (z. B. Sozialgesetzbuch Teil X, Meldegesetze, Verfassungsschutzgesetz NW u. a.) ist deshalb schon heute die historische Unterscheidung zwischen der Datenverarbeitung in Dateien und in Akten bereits ganz oder weitgehend aufgegeben. Eine solche Unterscheidung

entspricht auch nicht mehr dem Rechtsbewußtsein der Bürger: Alle Versuche, ihm den qualitativen Unterschied zwischen der Datenverarbeitung in Dateien und dem Umgang mit Daten in Akten deutlich zu machen und die damit bisher verbundenen völlig unterschiedlichen Rechtsfolgen zu erklären, sind im Ergebnis fehlgeschlagen; dies wird dadurch belegt, daß nachweisbar der größte Teil der Beschwerden über Verletzungen des Persönlichkeitsrechts Fälle betrifft, in denen es sich um die Verarbeitung personenbezogener Daten in Akten oder sonstigen Unterlagen handelt. Auch das Übereinkommen des Europarates vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten sieht in Kapitel I Artikel 3 Absatz 2c eine solche Erweiterung des Anwendungsbereichs der Datenschutzregelungen vor. Aus dem Gesichtspunkt der Einheit öffentlicher Informationsverarbeitung, nicht zuletzt auch im Interesse größerer Transparenz und Anwenderfreundlichkeit, soll der Datenschutz bei traditioneller Datenverarbeitung (in Akten) in das Datenschutzgesetz aufgenommen und nicht an anderer Stelle, etwa im Verwaltungsverfahrensgesetz, geregelt werden.

Mit der **Einbeziehung der traditionellen Informationsverarbeitung (Akten) in den Schutzzweck des Gesetzes** verliert der bisher für den Datenschutz zentrale Dateibegriff an Bedeutung. Selbst redaktionell unverändert bleibende bisherige Bestimmungen des Datenschutzgesetzes erhalten dagegen einen umfassenderen inhaltlichen Stellenwert, weil der Schutz des Gesetzes über den bisherigen Dateibegriff hinaus auf die herkömmliche Informationsverarbeitung in Akten ausgedehnt wird. Gleichwohl können und müssen Systematik und Begriffswelt des Gesetzes prinzipiell beibehalten werden; dies belegen gerade die wenig überzeugenden Versuche, die Verarbeitung personenbezogener Daten in Akten in einem eigenen Gesetz zu regeln. Damit ist jedoch nicht gesagt, daß der Schutz personenbezogener Daten ohne Rücksicht auf die Form der Datenverarbeitung unterschiedslos gewährleistet werden muß oder soll. Gegenüber der Datenverarbeitung in automatisierten Verfahren oder herkömmlichen Dateien sind für die manuelle Verarbeitung in Akten in technisch-organisatorischer Hinsicht, aber auch bei der Ausgestaltung der Rechte der Betroffenen differenzierte Regelungen vorgesehen.

Die der Wahrung des Rechts auf informationelle Selbstbestimmung dienenden **materiell-rechtlichen** und **verfahrensrechtlichen Vorschriften** des allgemeinen (und bereichsspezifischen) Datenschutzes und **die Kontrollbefugnis** des Landesbeauftragten für den Datenschutz sind **als Einheit** zu betrachten und müssen einander entsprechen. Aus der Erweiterung des Schutzzweckes des Datenschutzgesetzes folgt zwingend eine ebenso umfassend angelegte Kontrollbefugnis des Datenschutzbeauftragten. Mit der entsprechenden Einbeziehung jeglicher personenbezogener Informationsverarbeitung der öffentlichen Verwaltung werden auch seit Jahren bestehende teilweise unterschiedliche Auffassungen um den Umfang dieser Kontrollbefugnis endgültig ausgeräumt.

c) Das Recht auf **informationelle Selbstbestimmung** ist nur dann gewährleistet, wenn der Betroffene bewußt über **die Preisgabe und die Verwendung seiner persönlichen Daten entscheiden** kann. Er muß also wissen, für welche Zwecke er seine Angaben macht und welche Verarbeitungsmaßnahmen beabsichtigt sind. Denn nur unter diesen Voraussetzungen kann er die Konsequenzen seiner Auskunftserteilung abschätzen. Gerade im Stadium der Informationsgewinnung durch die Behörde besteht für den Betroffenen oft die einzig wirksame Möglichkeit, sein informationelles Selbstbestimmungsrecht auszuüben. Aus verfassungsrechtlichen Gründen soll deshalb die **Erhebung** personenbezogner Daten als geschützte Phase der Datenverarbeitung mit ihren jeweiligen Voraussetzungen in das Datenschutzgesetz einbezogen und die **Aufklärungs- und Belehrungspflichten** gegenüber dem Betroffenen entsprechend erweitert werden. Bei anderen Stellen oder Personen dürfen personenbezogene Daten nur unter den Voraussetzungen erhoben werden, unter denen eine Zweckänderung gespeicherter Daten zulässig wäre. Der **Datenverarbeitungsbegriff** soll im übrigen wie bisher durch bestimmte **Phasen** definiert werden; dazu soll in Zukunft auch jede **Nutzung** personenbezogener Daten zählen.

d) Grundlegende Bedeutung kommt im Rahmen der Novellierung des Datenschutzgesetzes der Einführung des **Zweckbindungsprinzips** zu. Bei der Hergabe seiner Daten vertraut der Bürger darauf oder muß darauf vertrauen können, daß diejenigen Umstände, die ihn zur Preisgabe seiner Daten veranlaßt haben, auch tatsächlich zutreffen und von der verarbeitenden Stelle beachtet werden. Dies gilt in erster Linie für die Weiterverarbeitung durch die erhebende Stelle selbst, aber auch für die Übermittlung dieser personenbezogenen Daten an andere Stellen oder Personen und ist auch bei der Erhebung von Bedeutung. Die dem Zweckbindungsprinzip entsprechenden Regelungen erfüllen wichtige präventive Schutzfunktionen zugunsten des Betroffenen beim Umgang mit personenbezogenen Daten durch die öffentliche Verwaltung. Als Konsequenz der Einführung der

Erhebungsphase wird deshalb die Weiterverarbeitung personenbezogener Daten durch die speichernde Stelle **grundsätzlich an den Erhebungszweck** gebunden. Eine anderweitige Weiterverarbeitung der Daten ist nur unter ganz bestimmten Ausnahmetatbeständen, die enumerativ aufgeführt werden, zulässig.

e) Einen weiteren **Schwerpunkt** des Entwurfes bilden die neuen Regelungen über das **Verhältnis** des **informationellen Selbstbestimmungsrechtes zur Amtshilfe (Informationshilfe)**. Nach den überkommenen Grundsätzen der Amtshilfe – die auch in den allgemeinen Datenschutzgesetzen ihren Niederschlag gefunden haben – ist die Übermittlung personenbezogener Informationen von einer öffentlichen Stelle an eine andere zulässig, wenn dies zur Erfüllung von Aufgaben der übermittelnden oder der empfangenden Stelle erforderlich ist. Mit der prinzipiellen Anerkennung der Zweckbindung erhobener Daten ist eine solche, allein in das pflichtgemäße Ermessen der Behörden gestellte Disposition über personenbezogene Daten nicht mehr zu vereinbaren. Der Entwurf strebt eine verfassungskonforme Lösung dieser schwierigen Problematik im Wege eines gesetzgeberischen Kompromisses an. Im Hinblick auf die unterschiedliche Sensitivität der für eine Datenübermittlung im Wege der Amtshilfe in Betracht kommenden personenbezogenen Daten und unter Berücksichtigung der nicht weniger differenzierten potentiellen Gefährdung des informationellen Selbstbestimmungsrechtes soll an die Stelle der bisherigen Generalklauseln eine stärkere Präzisierung, Konkretisierung und Einschränkung dieser allgemeinen Informationshilfeklauseln treten. Für Bereiche von insgesamt **besonderer** Sensitivität, etwa im Gesundheits- oder Sozialbereich, bedarf es besonderer, **bereichsspezifischer Regelungen,** die die Voraussetzungen und Grenzen einer zulässigen Datenübermittlung auch für den Bürger eindeutig erkennen lassen. Der Entwurf knüpft deshalb auch für die Übermittlung an das Zweckbindungsprinzip an und enthält darüber hinaus eine Verweisung auf die Ausnahmetatbestände dieses Grundsatzes, bei deren Vorliegen eine Übermittlung trotz der damit zwangsläufig verbundenen Zweckänderung erhobener personenbezogener Daten in Zukunft zulässig sein soll. Für den Bereich der Amtshilfe (Informationshilfe) kommt damit den generellen Amtshilfevorschriften des Verwaltungsverfahrensgesetzes nur noch ergänzende Bedeutung zu; für die **datenschutzrechtliche Zulässigkeit** einer Datenerhebung bei einer anderen öffentlichen Stelle oder einer entsprechenden Übermittlung an eine andere öffentliche Stelle ist **allein das Datenschutzgesetz** oder eine andere spezielle und insoweit vorrangige datenschutzrechtliche Regelung maßgeblich. Dies wird durch die gleichzeitige Änderung des Verwaltungsverfahrensgesetzes (s. Artikel 3 Nr. 1, § 3a Satz 2) klargestellt.

f) Die Aussagen des Bundesverfassungsgerichts zum informationellen Selbstbestimmungsrecht machen auch eine **Neustrukturierung des bisherigen Auskunftsrechtes** des Betroffenen unabweisbar. Prinzipiell soll in Zukunft der Grundsatz gelten: Jedermann kann unentgeltlich Auskünfte über seine personenbezogenen Daten bei allen speichernden öffentlichen Stellen einholen. Von dieser Auskunftsverpflichtung sollen auch nicht bestimmte Gruppen von Behörden ausgenommen sein. Nur in einigen wenigen Fällen soll die Auskunftserteilung unterbleiben, wenn die Aufgabenerfüllung der speichernden Stelle, gravierende öffentliche Interessen oder besondere Geheimhaltungsinteressen insbesondere von Dritten Vorrang beanspruchen müssen. Nur in besonderen Fällen darf auch von einer Begründung für die Auskunftsverweigerung abgesehen werden. Die wesentlichen Gründe sind bei der Auskunftsverweigerung oder unterbliebener Begründung intern zu dokumentieren.

   Sind die personenbezogenen Daten in Akten gespeichert, so soll darüber hinaus dem Betroffenen ein Einsichtsrecht gewährt werden, soweit dies möglich ist und sich nicht aus § 29 Verwaltungsverfahrensgesetz etwas anderes ergibt.

g) Die Vorschriften für die **Berichtigung, Sperrung und Löschung** von Daten sollen zwar im Prinzip beibehalten werden, bedürfen aber einiger Erweiterungen; die Position des Betroffenen soll z. B. durch eine **obligatorische Löschungsverpflichtung** verbessert werden. Dabei sind allerdings die Besonderheiten der aktenmäßigen Datenverarbeitung und die Belange des Archivwesens zu berücksichtigen.

h) Die **Voraussetzungen für** die erforderliche **interne bzw. externe Datenschutzkontrolle** sollen verbessert und zugleich vereinfacht werden: Zur Selbstkontrolle durch die speichernde Stelle soll in Zukunft für Dateien eine sog. **Dateibeschreibung** angelegt und vorgehalten werden. Die Anmeldepflicht zum **Register des Landesbeauftragten** für den Datenschutz soll sich auf alle automatisiert geführten Dateien erstrecken, für die eine Dateibeschreibung vorzuhalten ist. Die bisherige **Veröffentlichungspraxis** (Datenschutzveröffentlichungsverordnung NW vom 6. November 1979, GV. NW. S. 726) hat die in sie ursprünglich gesetzten Erwartungen nicht erfüllt und zu einem mehr und mehr aufwendigen Formalismus geführt; sie soll deshalb entfallen.

i) Das besondere Gefährdungspotential von **Direktzugriffsverfahren** (On-line-Verbindungen) gebietet es, für den Bereich der öffentlichen Stellen des Landes On-line-Verbindungen nur aufgrund einer Rechtsvorschrift zuzulassen; darüber hinaus sind besondere Zulässigkeitsvoraussetzungen und technisch/organisatorische Maßnahmen vorgesehen. Dies soll entsprechend auch für regelmäßige Datenübermittlungen gelten.

j) Ein eigener Abschnitt ist verschiedenen **datenschutzrechtlichen Sonderbestimmungen** gewidmet, die gleichwohl von genereller Bedeutung sind.

Die Regelung über die Zulässigkeit der Datenverarbeitung für wissenschaftliche Zwecke (sog. Wissenschaftsklausel, bisher § 12 DSG NRW) wird völlig neu gefaßt. Darüber hinaus regelt der Entwurf erstmals die Datenverarbeitung bei Dienst- und Arbeitsverhältnissen im öffentlichen Bereich. Auch für das Fernmessen und Fernwirken ist eine Regelung vorgesehen. Die Zulässigkeit der Nutzung personenbezogener Verwaltungsdaten zu statistischen Zwecken durch die öffentlichen Stellen und die Nutzung von Einzelangaben aus der amtlichen Statistik durch Gemeinden und Gemeindeverbände werden ebenfalls in dem Entwurf behandelt. Sonderbestimmungen über die Datenverarbeitung durch den Westdeutschen Rundfunk Köln enthält der Entwurf nicht, weil solche Regelungen Bestandteil des Gesetzes über den Westdeutschen Rundfunk – WDR-Gesetz – vom 19. 3. 1985 (GV. NW. S. 237) geworden sind. Eine Klarstellung bezüglich der Kontrollorgane sieht Art. 5 durch entsprechende Änderung des WDR-Gesetzes vor.

k) Der Gesetzentwurf sieht die Aufhebung der bisherigen Sonderbestimmungen im 3. Abschnitt des Datenschutzgesetzes bezüglich der **kommunalen Eigenbetriebe und öffentlich-rechtlichen Wettbewerbsunternehmen** vor. Da diese landesrechtlichen Vorschriften fast vollständig den Vorschriften des 3. Abschnitts des Bundesdatenschutzgesetzes (Datenverarbeitung nicht-öffentlicher Stellen für eigene Zwecke) entsprechen, erscheint es – auch zur Entlastung des Datenschutzgesetzes von entbehrlichen Vorschriften – geboten, diese Sondervorschriften aufzuheben; die Eigenbetriebe und öffentlich-rechtlichen Wettbewerbsunternehmen, soweit sie in dieser Eigenschaft im Rechtsverkehr teilnehmen, werden im Interesse einer Gleichbehandlung mit der Privatwirtschaft unmittelbar auf die entsprechenden Vorschriften des Bundesdatenschutzgesetzes (3. und 4. Abschnitt) verwiesen. Die Kontrollbefugnis des Landesbeauftragten sowie die Geltung besonderer Vorschriften über den Datenschutz bleiben davon unberührt.

l) Die **Straf- und Bußgeldvorschriften** sollen inhaltlich neu strukturiert und die Tatbestände deutlicher gegeneinander abgegrenzt werden. Eine Kriminalisierung der Datenverarbeitung soll dabei vermieden werden.

Trotz der Bemühungen, den bestehenden Aufbau möglichst beizubehalten, ist eine **teilweise Neustrukturierung des Gesetzes** unvermeidbar. Dies erzwingt schon der vorgesehene Fortfall des 3. Abschnittes, umgekehrt aber auch die Einführung der datenschutzrechtlichen Sonderregelungen.

Schließlich sollen umfängliche redaktionelle Verbesserungen den Zugang zum Datenschutzgesetz erleichtern, zu mehr Rechtsklarheit und -sicherheit in der Anwendung beitragen und damit den Datenschutz insgesamt bürgerfreundlicher machen. Die vorgesehenen **Änderungen** erreichen insgesamt einen solchen Umfang, daß eine **Neufassung des Datenschutzgesetzes** erforderlich ist.

B Im einzelnen

Zur Änderung der Gesetzesüberschrift und zu § 1 (Aufgabe)

Die Neufassung der Gesetzesüberschrift und des § 1 entspricht dem akzentuierteren verfassungsrechtlichen Ansatz; sie verdeutlicht die Erweiterung des Schutzzweckes des Gesetzes. Das Datenschutzgesetz will nicht mehr allein den Mißbrauch bei der dateimäßigen, insbesondere automatisierten Verarbeitung personenbezogener Daten verhindern; vielmehr sollen generelle Regelungen für den Umgang mit personenbezogenen Daten im öffentlichen Bereich geschaffen werden. Gewährleistet sein soll der Schutz des Bürgers vor möglichen Gefährdungen oder Beeinträchtigungen seines informationellen Selbstbestimmungsrechts, die sich aus der bloßen Informationsverarbeitung durch die öffentliche Verwaltung ergeben können. Die Verhinderung von Mißbrauch kann nur eine **Folge** dieser Regelungen und nicht ihr Ausgangspunkt und Maßstab sein. Ohnehin lassen die vielfältigen Verwendungs- und Verknüpfungsmöglichkeiten der automatisierten Datenverarbeitung keine sichere Voraussage mehr zu, welche Sachverhalte die Gefahr eines Mißbrauchs in sich bergen.

Die vorgesehene Neuformulierung der Gesetzesaufgabe in § 1 Nr. 1 entspricht der Definition des Rechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht in seiner Entscheidung vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 (BVerfGE 65, 1); dies wird auch durch den Klammerzusatz deutlich. Das informationelle Selbstbestimmungsrecht wird aber nur insoweit geschützt, als eine „unzulässige Beeinträchtigung" dieses Rechts erfolgt. Grundsätzlich muß der einzelne nämlich Einschränkungen seines Rechts auf informationelle Selbstbestimmung im Allgemeininteresse hinnehmen. Diese Beschränkungen bedürfen aber einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Eingriffe für den Betroffenen erkennbar ergeben (vgl. Artikel 4 Abs. 2 LV). Die Schaffung solcher Rechtsgrundlagen gehört – unbeschadet der Notwendigkeit modifizierender oder ergänzender Sonderregelungen für einzelne Verwaltungsbereiche – zu den wesentlichen Aufgaben dieses Gesetzes. Insofern bleibt dem Datenschutzgesetz nach wie vor die Funktion, grundsätzlich den verfassungsrechtlich gebotenen Ausgleich zwischen den Belangen des Betroffenen und gegenläufigen Interessen der verarbeitenden Stellen und anderer Nutzer der Datenverarbeitung sicherzustellen. Inwieweit danach Eingriffe in das informationelle Selbstbestimmungsrecht durch die Verarbeitung personenbezogener Daten zulässig sind, wird aber nicht ausschließlich abstrakt, sondern unter Berücksichtigung der Aufgaben und der Zwecke, denen die Verarbeitung bestimmter personenbezogener Daten dient, geregelt. Geschützt werden soll auch nicht nur – wie nach dem bisherigen Wortlaut – der „Bürger", wie ihn etwa die Gemeindeordnung kennt, sondern jeder „einzelne".

Nach § 1 Nr. 2 soll das verfassungsgemäße Gefüge nunmehr vor einer „Gefährdung" statt vor einer bloßen „Veränderung" durch die automatisierte Datenverarbeitung bewahrt werden; die Vorschrift steht in Zusammenhang mit § 22 Absatz 2 (bisher § 26 Absatz 4).

Der bisherige Absatz 2 wird in veränderter Form § 2 Absatz 1 des Entwurfs; der frühere Absatz 3 ist bereits im Zusammenhang mit dem Gesetz über den Westdeutschen Rundfunk – WDR-Gesetz – vom 19. 3. 1985 (GVBl. S. 237) aufgehoben worden.

Zu § 2 (Anwendungsbereich)

Abweichend von der bisherigen Regelung in § 1 Absatz 2 wird der Anwendungsbereich des Gesetzes künftig in einer eigenen Vorschrift geregelt, weil dieser Frage als Folge der erheblichen Erweiterung des gesetzlichen Schutzzwecks ein besonderes Gewicht zukommt. Eine eigene Vorschrift empfiehlt sich auch aus Gründen der besseren Verständlichkeit.

Die Normadressaten in Absatz 1 Satz 1 entsprechen dem bisherigen Recht; wegen des erweiterten Anwendungsbereichs kann der Wortlaut dieser Bestimmung gestrafft werden. Die bisher in § 1 Absatz 2 Satz 1 aufgeführten Behörden, Einrichtungen und sonstigen Stellen im Landes- und Kommunalbereich werden aus Gründen der besseren Übersichtlichkeit des Gesetzes als „öffentliche Stelle" definiert, so daß die bisher zahlreichen Verweisungen vermieden werden können. Dazu gehören – wie bisher – auch Vereinigungen öffentlicher Träger in Privatrechtsform soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen (vgl. § 22 Abs. 3 BDSG) sowie öffentlich bestellte Vermessungsingenieure. Wie bisher soll dieses Gesetz auf die Gerichte und Behörden der Staatsanwaltschaft nur anwendbar sein, soweit diese Verwaltungsaufgaben erledigen. Als Organe der Rechtspflege unterliegen sie gemäß § 7 Abs. 2 Satz 1 BDSG dem Bundesdatenschutzgesetz, soweit sich nicht aus speziellen Verfahrensgesetzen des Bundes etwas anderes ergibt. Durch den gleichzeitig vorgeschlagenen Wegfall des § 32 (Sonderbestimmung für die Gerichte) wird klargestellt, daß auch die Behörden der Staatsanwaltschaft – ebenso wie die Gerichte – der Kontrolle des Landesbeauftragten für den Datenschutz nur insoweit unterliegen, als sie Verwaltungsaufgaben wahrnehmen; dies entspricht der bisherigen Auffassung. Der Landtag fällt nur in den Anwendungsbereich des Datenschutzgesetzes, soweit er Verwaltungsaufgaben erledigt.

Nach Absatz 1 Satz 2 wird die Ausübung des Gnadenrechts wegen der nicht vergleichbaren Besonderheiten dieses Verfahren aus dem Anwendungsbereich des Gesetzes herausgenommen.

Die wesentlichste materielle Erweiterung liegt in der Einbeziehung der Verarbeitung personenbezogener Daten in bzw. aus Akten. Prinzipiell unabhängig von der jeweiligen Form der Verarbeitung (dateimäßig/nicht dateimäßig, automatisiert oder konventionell) soll der Umgang mit personenbezogenen Daten durch die öffentliche Verwaltung in den Schutzzweck des Gesetzes einbezogen werden. Die verschiedenen Formen der Datenverarbeitung werden jedoch nicht ausnahmslos denselben Bestimmungen unterworfen; Differenzierte Regelungen sollen der jeweiligen Art der Datenverarbeitung Rechnung tragen. Auf diese Weise werden der Schutz des informationellen Selbstbestimmungsrechts und die Modalitäten des unterschiedlichen Verwaltungsvollzugs sachgerecht gegeneinander abgewogen; die betreffenden Fälle ergeben sich jeweils unmittelbar aus den einzelnen Vorschriften. Der Begriff „Akte" ist in § 3 Absatz 5 definiert.

Für die kommunalen Eigenbetriebe, bestimmte öffentliche Einrichtungen und sonstige öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, sollen nach Absatz 2 Sätze 1 und 2 für die Datenverarbeitung im Rahmen wirtschaftlicher Zwecke in Zukunft grundsätzlich die für Wirtschaftsunternehmen des Privatrechts geltenden Vorschriften des Bundesdatenschutzgesetzes – BDSG – (Dritter/Vierter Abschnitt) unmittelbar Anwendung finden; die Unternehmen sollen allerdings nach wie vor den Vorschriften des Zweiten Teils dieses Gesetzes und damit der Kontrolle des Landesbeauftragten für den Datenschutz unterliegen. Darüber hinaus werden sie dem § 8 (Dateibeschreibung) und den besonderen Datenschutzregelungen aus dem Dritten Teil dieses Gesetzes unterworfen.

Im einzelnen gilt:

Die bisherigen Vorschriften der §§ 18 bis 23 (sog. Sonderbestimmungen für Eigenbetriebe und öffentlich-rechtliche Unternehmen), die fast ausnahmslos wörtlich den Regelungen des Bundesdatenschutzgesetzes (Dritter Abschnitt) entsprechen, sollen entfallen. Die Aufhebung dieser nahezu identischen landesrechtlichen Regelung zugunsten einer Verweisung auf die materiellen Bestimmungen des Bundesdatenschutzrechts erscheint geboten, weil kein überzeugender Grund besteht, die kommunalen Eigenbetriebe, sonstigen Einrichtungen und öffentlich-rechtlichen Unternehmungen generell anders zu behandeln als die privaten Unternehmen, mit denen sie im Wettbewerb stehen. Überdies ist davon auszugehen, daß auch die für die private Wirtschaft geltenden Vorschriften des Bundesdatenschutzgesetzes durch eine Novellierung Verbesserungen erfahren. Eine uneingeschränkte Verweisung auf das Bundesrecht hätte allerdings auch die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten zur Folge; dies erscheint im Hinblick auf die Kontrolle durch den Landesbeauftragten für den Datenschutz entbehrlich.

Soweit für bestimmte Unternehmen besondere Datenschutzbestimmungen (z. B. im medizinischen oder sozialen Bereich) bestehen, sind diese Vorschriften ohnehin vorrangig zu beachten.

Für die Eigenbetriebe und öffentlich-rechtlichen Wettbewerbsunternehmen sollen auch § 8 (Dateibeschreibung) und die besonderen Vorschriften für die Datenverarbeitung für wissenschaftliche Zwecke (§ 28) und bei Dienst- und Arbeitsverhältnissen (§ 29) sowie über das Fernmessen und Fernwirken (§ 30) und die Nutzung von Verwaltungsdaten zu statistischen Zwecken (§ 31) Anwendung finden, weil insoweit für eine unterschiedliche Behandlung dieser Unternehmen gegenüber den übrigen öffentlichen Stellen keine Veranlassung besteht.

Nach Absatz 2 Satz 3 wird für die Zukunft klargestellt, daß auch Schulen in kommunaler Trägerschaft, soweit sie personenbezogene Daten in inneren Schulangelegenheiten verarbeiten, ebenfalls als öffentliche Stellen im Sinne des Absatzes 1 Satz 1 anzusehen sind. Sie sind damit speichernde Stelle und unterliegen der Anmeldungspflicht zum Dateienregister nach § 23; zugleich tritt damit eine entsprechende Entlastung bei den kommunalen Trägern ein.

Absatz 3 enthält eine klarstellende Regelung für das Verhältnis zwischen den Bestimmungen des Datenschutzgesetzes Nordrhein-Westfalen gegenüber sonstigen „bereichsspezifischen" Datenschutzvorschriften; eine entsprechende Regelung enthielt bisher schon § 37. Das Datenschutzgesetz Nordrhein-Westfalen als allgemeine Datenschutzregelung ist ein Auffanggesetz, das gegenüber spezialgesetzlichen Regelungen subsidiär ist. Dies gilt nicht nur für spezielle bundesrechtliche Regelungen, sondern auch für Fachgesetze des Landes, soweit diese Regelungen für den Umgang mit personenbezogenen Daten enthalten. Als allgemeines Ausführungsgesetz zu Artikel 4 Absatz 2 Landesverfassung regelt das Datenschutzgesetz diejenige Datenverarbeitung, die mangels besonderer Eingriffstiefe keiner bereichsspezifischen Norm bedarf. Für das Verhältnis zum Verwaltungsverfahrensgesetz für das Land Nordrhein-Westfalen (VwVfG NW) enthält Artikel 3 Nr. 1 (§ 3a Satz 2) eine klarstellende Regelung dahingehend, daß die Behörden – auch im Verwaltungsverfahren – uneingeschränkt den Bestimmungen des Datenschutzgesetzes unterliegen, soweit sie im Sinne dieses Gesetzes personenbezogene Daten verarbeiten oder nutzen. Eine Ausnahme gilt nur im Verhältnis der Vorschrift des § 18 DSG NW (Akteneinsichtsrecht) zu § 29 VwVfG NW (vgl. Artikel 1 § 18 Absatz 2 Satz 2).

Zu § 3 (Begriffsbestimmungen)

Die Vorschrift soll aus Gründen der Übersichtlichkeit künftig alle für das Datenschutzgesetz wesentlichen Begriffsbestimmungen enthalten. Die bisherigen Regelungen sind unter Berücksichtigung des Rechts auf informationelle Selbstbestimmung zum Teil erweitert oder neuformuliert worden.

In Absatz 1 wird der bisherige Begriff der „Einzelangabe" beibehalten. Damit sind alle Angaben über persönliche und sachliche Verhältnisse gemeint, die über eine natürliche Person etwas aussagen, unabhängig davon, in welcher technischen Form (z. B. Bildaufnahme) dies geschieht. Der Begriff hält die Einbeziehung neuer technischer Verfahren in das Gesetz offen.

Absatz 2 sieht eine bedeutsame Erweiterung des bisher auf vier Phasen (Speichern, Verändern, Übermitteln und Löschen) beschränkten Datenverarbeitungsbegriffs vor und bezieht dabei die Nutzung mit ein. Nach wie vor kommt der Legaldefinition einzelner Verarbeitungsphasen Bedeutung zu, weil nicht darauf verzichtet werden kann, für sie im Gesetz besondere Zulässigkeitsanforderungen vorzugeben. Eine vollständige Aufgabe dieser Phasen ist daher nicht möglich und auch nicht erforderlich. Um für den Umgang mit personenbezogenen Daten keine Regelungslücke zuzulassen, soll in Satz 1 auch die (sonstige) Nutzung personenbezogener Daten im Sinne jedweder Verwendung als besondere Phase definiert und den übrigen Phasen gleichgestellt werden. Auch das Bundesverfassungsgericht bindet das Recht auf informationelle Selbstbestimmung nicht an bestimmte Phasen der Datenverarbeitung, sondern spricht allgemein von der „Verwendung" personenbezogener Daten.

In Absatz 2 Satz 2 Nr. 1 soll künftig die Erhebung als neue Datenverarbeitungsphase definiert und in den Schutzzweck des Gesetzes einbezogen werden. Das Recht, selbst über die Preisgabe und Verwendung persönlicher Daten bestimmen zu dürfen, ist gerade am Beginn der Datenverarbeitung von grundlegender Bedeutung. Der Begriff umfaßt nicht die zufällig erlangten oder aufgedrängten Informationen, für die aber Regelungen über die Zweckbindung gelten sollen (vgl. § 13 Absatz 1 Satz 3). Der Entwurf geht – verfassungskonform – in erster Linie vom Beschaffen personenbezogener Daten beim Betroffenen selbst aus, muß jedoch bei der Unterschiedlichkeit der Aufgabenstellung auch andere Formen der Informationsbeschaffung miteinbeziehen. Die der Behörde zugewiesene Tätigkeit kann es erforderlich machen, Informationen bei anderen Stellen oder Personen zu beschaffen. Grundsätzlich soll dies unter den gleichen Voraussetzungen zulässig sein, unter denen erhobene personenbezogene Daten zweckentfremdet werden dürfen (§ 12 Absatz 1 Satz 3, 2. Halbsatz i.V.m. § 13 Absatz 2 Satz 1). Das Erheben umfaßt folglich jede Form gezielt betriebener Gewinnung personenbezogener Daten unter Mitwirkung des Betroffenen, anderer Behörden oder privater Dritter sowie durch zweckgerichtete Beobachtung.

Der Speicherungsbegriff in Satz 2 Nr. 2 ist dem nunmehr umfassenden Begriff der „Verarbeitung" redaktionell angeglichen worden.

In Satz 2 Nr. 4 wird der Übermittlungsbegriff teilweise neugefaßt. Bisher gilt neben der Weitergabe der Daten bereits das Bereithalten von Daten zum Abruf als Übermittlung. Die damit beabsichtigte „Vorverlegung" des Datenschutzes bei automatisierten Direktabrufverfahren erweist sich aber auf der Grundlage der geltenden allgemeinen Übermittlungsvorschriften als nicht praktizierbar. Da für das automatisierte Direkabrufverahren nunmehr in § 9 besondere Zulässigkeitsvoraussetzungen vorgesehen sind, besteht keine Notwendigkeit mehr, bereits im Bereithalten von Daten eine Übermittlung anzunehmen; für die Einsichtnahme (Schlüssellösung) verbleibt es aber bei der bisherigen Regelung. Die Neuregelung beim Direktabrufverfahren beinhaltet auch eine den tatsächlichen Verfügungsmöglichkeiten der beteiligten Stellen entsprechende Regelung der datenschutzrechtlichen Verantwortlichkeit beim einzelnen Übermittlungsvorgang (vgl. § 14 Absatz 3 Satz 4).

In Satz 2 Nr. 5 wird auch die Sperrung als zusätzliche Datenverarbeitungsphase definiert. In Satz 2 Nr. 7 wird auch jede Verwendung personenbezogener Daten als Nutzen (Nutzung) von Daten definiert und den sonstigen Datenverarbeitungsphasen gleichgestellt.

Die übrigen Begriffsbestimmungen in Absatz 2 Satz 2 entsprechen dem bisherigen Recht. In Absatz 2 Satz 2 Nr. 4 wurde ebenso wie in Absatz 3 der Begriff „speichernde" Stelle durch „datenverarbeitende" Stelle ersetzt. Damit soll klargestellt werden, daß dem Gesetz auch solche Stellen unterliegen, die selbst keine Daten speichern, sondern nur über ein Sichtgerät abrufen und verwerten.

Die bisher in Absatz 3 Nr. 1 enthaltene Definition der „speichernden Stelle" ist entbehrlich, weil sich diese Begriffsbestimmung bereits aus Absatz 2 Satz 2 Nr. 2 herleiten läßt. Für den Fall der Auftragsdatenverarbeitung ist überdies in § 11 Absatz 1 Satz 2 klargestellt, daß der Auftraggeber als „speichernde Stelle" anzusehen ist.

Der Absatz 3 ist im übrigen auch aus Gründen besserer Lesbarkeit teilweise neugefaßt.

Absatz 4 enthält eine neue und vereinfachte Definition des Dateibegriffs (bisher Absatz 3 Nr. 3). Da die Anwendbarkeit des Gesetzes nicht mehr allein vom Dateibegriff abhängt, wird dieser zwar an Bedeutung verlieren. Als Anknüpfungspunkt für bestimmte Folgeregelungen ist er jedoch von Bedeutung und bedarf daher der Legaldefinition zur Abgrenzung von der konventionellen Datenverarbeitung in und aus Akten. In Zukunft soll stärker zwischen automatisierter und nicht-automatisierter Verarbeitung unterschieden werden, an die teilweise auch unterschiedliche Rechtsfolgen anknüpfen: Grundsätzlich fallen alle Sammlungen von personenbezogenen Daten, die – unabhängig von der Art der Speicherung – in automatisierten Verfahren ausgewertet werden können, unter den Dateibegriff (automatisierte Datei). Nicht mehr wird gefordert, daß solche Datensammlungen gleichartig aufgebaut sein müssen, da durch

diese Beschränkung neue Verfahren wie der Bildschirmtext nicht erfaßt werden. Zu einer auswertbaren automatisierten Datensammlung zählen aber weder Fernkopierer, da sie keine Datensammlung enthalten, noch Schreibautomaten, soweit mit ihnen keine Daten ausgewertet werden können. Dadurch sind solche Verfahren, die aufgrund ihrer Verwendungsmöglichkeiten und ihrer Zweckbestimmung zu keiner Beeinträchtigung des informationellen Selbstbestimmungsrechts führen können, von der Anwendung des Gesetzes ausgenommen, ohne daß es dazu einer ausdrücklichen Regelung bedarf. Dem verarbeitungstechnisch geprägten Dateibegriff werden diejenigen nicht-automatisierten Datensammlungen gleichgestellt, die – wie bisher – gleichartig aufgebaut sind und nach bestimmten Merkmalen geordnet und ausgewertet werden können (nicht-automatisierte Datei). Dieser Dateibegriff ist damit gegenüber der sonstigen nicht-automatisierten Datenverarbeitung (konventionelle oder manuelle Verarbeitung in Akten, abgegrenzt. Die in Zukunft nur noch maßgeblichen materiellen Kriterien der Datenordnung und Datenauswertung (oder die Möglichkeit dazu) verdeutlichen, daß auf das besondere Gefährdungspotential solcher gleichartig aufgebauter Datensammlungen abgestellt wird.

In den Anwendungsbereich des Gesetzes werden nunmehr grundsätzlich auch diejenigen nicht-automatisierten Dateien einbezogen, aus denen keine personenbezogenen Daten übermittelt werden sollen (sog. interne Karteien), weil bereits Erhebung und Speicherung solcher Daten Eingriffe in das informationelle Selbstbestimmungsrecht darstellen können, selbst wenn (ursprünglich) keine Übermittlung beabsichtigt ist. Auch Daten, die nur zum internen Gebrauch gespeichert werden, können Grundlage für Entscheidungen sein, die den Betroffenen belasten.

Akten und Aktensammlungen erfüllen in der Regel den Dateibegriff nicht. Sind jedoch die Voraussetzungen des Absatzes 4 Buchst. a oder b ausnahmsweise erfüllt, sind sie als Datei zu behandeln, weil es auf die Art der Speicherung der personenbezogenen Daten nicht ankommt.

Der Aktenbegriff in Absatz 5 umfaßt nicht nur die Zusammenfassung von Unterlagen in einem Ordner, sondern jede einzelne amtliche oder dienstliche Unterlage, soweit sie für die Erfüllung einer öffentlichen Aufgabe bestimmt ist, im Regelfall also als Grundlage für konkrete Verwaltungsmaßnahmen dient. Dazu gehören auch Tonbänder, Filme und Fotos. Nicht unter den Begriff der „Akte" fallen jedoch Vorentwürfe oder persönliche Notizen des Bearbeiters, es sei denn, daß sie Bestandteil eines Vorgangs werden und damit amtlichen Charakter erhalten.

Bei konventioneller Verarbeitung personenbezogener Daten in bzw. aus Akten handelt es sich gegenüber der automatisierten Datenverarbeitung oft nicht um ausschließlich auf eine bestimmte Person bezogene Einzelinformationen, sondern um personenbezogene Angaben, die untrennbar mit anderen Daten verbunden sind, so daß die an sich gebotene beschränkte Übermittlung, Auskunft oder Korrektur bestimmter Daten in der Regel nicht möglich ist, ohne den inneren oder äußeren Sachzusammenhang der Informationen zu zerstören. Bestimmte Pflichten datenverarbeitender Stellen können daher nicht mit den gleichen Methoden verwirklicht werden, wie dies bei der Datenverarbeitung in automatisierten Verfahren möglich ist. Bei der aktenmäßigen Datenverarbeitung sind daher einige „Abstriche" unvermeidbar, weil sich nur so sachgerechte und überzeugende Ergebnisse erzielen lassen.

Zu § 4 (Zulässigkeit der Datenverarbeitung)

Die neugefaßte Vorschrift enthält in Satz 1 – bisher § 3 Satz 1 – die allgemeinen Zulässigkeitsvoraussetzungen jedweder Verarbeitung personenbezogener Daten (im Sinne des § 3 Absatz 2) durch die öffentliche Verwaltung.

Die Sätze 2 und 3 des bisherigen § 3 wurden inhaltlich erweitert und dabei redaktionell überarbeitet. Die der öffentlichen Verwaltung auferlegten verstärkten Aufklärungspflichten verbessern den Schutz des Betroffenen bei freiwilligen Angaben und entsprechen damit dem Anliegen des informationellen Selbstbestimmungsrechts. Der Betroffene ist nicht nur in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären, sondern auch über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung auch über den Empfänger der Daten, er ist unter Hinweis auf die Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann.

Zu § 5 (Rechte des Betroffenen)

In Satz 1 werden in Katalogform die Rechte des Betroffenen zwecks besserer Information des einzelnen zusammengefaßt. Bis auf den Fortfall der Nr. 6 und die Erweiterung in Nr. 1 handelt es sich im wesentlichen um eine redaktionelle Überarbeitung und Straffung des bisherigen § 4 Absatz 1.

Die Voraussetzungen, unter denen die aufgeführten Rechte wahrgenommen werden können, ergeben sich aus den jeweils angegebenen Einzelvorschriften.

Der bisher in § 4 Absatz 1 Nr. 6 gegebene Unterlassungs- bzw. Folgenbeseitigungsanspruch entfällt. Voraussetzung für beide Ansprüche war zunächst, daß personenbezogene Daten bei der speichernden Stelle trotz erfolgter Berichtigung, Sperrung oder Löschung in irgendeiner Weise weiter genutzt und dadurch schutzwürdige Belange des Betroffenen beeinträchtigt wurden. Diese Weiternutzung mußte dabei in anderer Weise als im Zusammenhang mit einer erneuten Speicherung bzw. Übermittlung aus Dateien geschehen, weil sonst die primären Rechte auf Berichtigung, Sperrung und Löschung wieder zur Anwendung gekommen wären. Der Unterlassungs- bzw. Folgenbeseitigungsanspruch ging deshalb über den bisher durch § 2 begrenzten Anwendungsbereich des Datenschutzgesetzes hinaus (überschießende Tendenz). Mit der Einbeziehung der Nutzung in den Schutzzweck des Gesetzes entfällt die Notwendigkeit für eine solche Regelung, weil der Betroffene seine Rechte in Zukunft gegenüber jeder Form der Verwendung personenbezogener Daten durch die öffentliche Verwaltung geltend machen kann.

Die Voraussetzungen des bisher in § 4 Absatz 2 enthaltenen Schadensersatzanspruchs werden in § 20, im Dritten Abschnitt des Gesetzes, neu geregelt.

Der neue Satz 2 stellt sicher, daß diese Rechte des Betroffenen unter keinen Umständen, auch nicht durch Einwilligung des Betroffenen, ausgeschlossen oder beschränkt werden können.

Zu § 6 (Datengeheimnis)

Neben inhaltlichen Präzisierungen und redaktionellen Verbesserungen entfällt die bisher in § 5 Absatz 2 Satz 1 vorgesehene förmliche Verpflichtung auf das Datengeheimnis. Diese Verpflichtung erscheint in der öffentlichen Verwaltung nach den Erfahrungen der Praxis entbehrlich; sie hat zu erheblichem Verwaltungsaufwand geführt, ohne den Schutz des Persönlichkeitsrechts zu stärken. Die Vorschrift kann deshalb auch aus Gründen der Entbürokratisierung entfallen. Die materiellen datenschutzrechtlichen Verpflichtungen der Personen, die dienstlichen oder sonst berechtigten Zugang zu personenbezogenen Daten haben, bleiben unberührt.

Zu § 7 (Sicherstellung des Datenschutzes)

Die – gekürzte – Vorschrift entspricht im wesentlichen der bisherigen Regelung in § 8 Satz 1; sie enthält die allgemeine Verpflichtung und Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften. Diese Verpflichtung ist Teil der generellen Pflicht dieser Stellen, die Rechtmäßigkeit und Ordnungsmäßigkeit der ihnen unterstellten Verwaltung zu gewährleisten.

Die bisher in Satz 1 nur mittelbar ausgesprochene Verpflichtung der Verwaltung, die „Grundsätze" der (externen) Datenübermittlung an andere Behörden und sonstige Stellen auch beim internen Datenfluß zu beachten, darf in dieser eher beiläufigen Form in Hinblick auf das informationelle Selbstbestimmungsrecht nicht belassen werden. Die interne Datenweitergabe muß vielmehr wegen des durchaus vergleichbaren Gefährdungspotentials grundsätzlich den gleichen Zulässigkeitsanforderungen unterworfen werden wie die (externe) Datenübermittlung (vgl. Zu § 14 Absatz 5).

Auch die bisher in § 8 Satz 2 Nrn. 1 und 2 angesprochenen besonderen Datenschutzmaßnahmen sollen an dieser Stelle entfallen; sie gehören künftig zu den Verpflichtungen zur Vorhaltung der Dateibeschreibung (vgl. Zu § 8).

Der bisherige § 9 (Allgemeine Verwaltungsvorschriften) soll ersatzlos entfallen. Der Normgehalt dieser Bestimmung, die bisher keine praktische Bedeutung erlangt hat, liegt in der Verpflichtung der obersten Landesbehörden, jeweils für ihren Geschäftsbereich allgemeine Verwaltungsvorschriften zur Ausführung des Datenschutzgesetzes zu erlassen. Es gehört jedoch ohnehin zum anerkannten Recht der Exekutive, unterhalb von Gesetz und Rechtsverordnung ergänzende verwaltungsinterne Regelungen zu erlassen. Einer besonderen Ermächtigung bedarf es dazu nicht. Datenschutzrechtliche Regelungen von Gewicht bleiben überdies dem Gesetz- oder Verordnungsgeber vorbehalten.

Zu § 8 (Dateibeschreibung)

Die bereits bisher nach § 8 Satz 2 Nrn. 1 und 2 vorzuhaltende Dateiübersicht und die vorgeschriebene Überwachung der Verarbeitungsprogramme werden wegen ihrer Bedeutung in einer neukonzipierten Vorschrift geregelt.

Nach Absatz 1 sind prinzipiell für jede Datei (gestaffelt von der nicht-automatisierten bis zur automatisierten Datei) Angaben vorzuhalten, die einerseits die Selbstkontrolle der speichernden Stelle sicherstellen, aber auch die Fremdkontrolle durch den Landesbeauftragten für den Datenschutz ermöglichen. Die Dateibeschreibung ist ferner ein wichtiges Hilfsmittel im Rahmen der Auskunftspflicht der Behörde. Die neue Regelung erweitert den Umfang der bisherigen Verpflichtungen, um das informationelle Selbstbe-

stimmungsrecht noch besser zu sichern. Der Pflicht zur Vorhaltung der Dateibeschreibung entspricht zugleich für automatisierte Verfahren die Meldepflicht zu dem beim Landesbeauftragten für den Datenschutz zu führenden Dateienregister (vgl. Zu § 23). Nach Absatz 2 gilt aber die Verpflichtung zur Vorhaltung einer Dateibeschreibung nicht für interne nicht automatisierte Dateien sowie automatisierte Dateien, die nach ihrer Zweckbestimmung von vornherein aus technischen Gründen nur vorübergehend vorgehalten werden, insbesondere Zwischen- oder Hilfsdateien. In diesen Fällen besteht kein Bedürfnis zur Einhaltung formeller Vorschriften, weil Beeinträchtigungen nicht zu befürchten sind.

Zu § 9 (Automatisiertes Abrufverfahren und regelmäßige Datenübermittlungen)

Den Verfahren zur automatisierten Direktabfrage von personenbezogenen Datenbeständen (On-line-Anschlüsse) als Informationsaustausch kommt unter den Aspekten des Datenschutzes und der Datensicherung besondere Bedeutung zu, weil die abrufende Stelle nach Einrichtung eines solchen Anschlusses über den gesamten Bestand der von der speichernden Stelle bereitgehaltenen Daten verfügen kann. Die mögliche Übermittlung einer sehr umfangreichen Anzahl personenbezogener Daten birgt erhebliche Gefahren für das informationelle Selbstbestimmungsrecht in sich. Überdies stellt der in § 3 Absatz 2 Satz 2 Nr. 4 neugefaßte Übermittlungsbegriff insoweit nicht mehr auf das Bereithalten ab, sondern auf den realen Abruf solcher Datenbestände. Wegen dieser Änderung und der besonderen Risiken der On-line-Anschlüsse wird die Einrichtung solcher Verfahren an besondere Zulässigkeitsvoraussetzungen gebunden.

Nach Absatz 1 wird in der öffentlichen Verwaltung (Landes- und Kommunalverwaltung) die Einrichtung derartiger automatisierter Abrufverfahren prinzipiell nur durch Bundes- oder Landesrecht zugelassen; die Einrichtung solcher Verfahren wird nicht dem Ermessen und der Einzelabwägung der beteiligten Behörden überlassen. Nicht betroffen sind danach On-line-Anschlüsse, mit denen nicht personenbezogene (statistische) Einzelangaben übermittelt werden. Absatz 1 findet ferner keine Anwendung auf diejenigen Fälle, in denen Behörden als Auftraggeber im Rahmen der Auftragsdatenverarbeitung ihre personenbezogenen Datenbestände bei Auftragnehmern (Rechenzentren) abrufen.

Nach Absatz 2 Satz 1 werden die Ressorts ermächtigt, für ihren Geschäftsbreich automatisierte Abrufverfahren durch Rechtsverordnung einzuführen. Vorbild für diese Regelungen sind Bestimmungen im Meldegesetz Nordrhein-Westfalen über den Datenaustausch. Voraussetzung ist, daß die Einrichtung solcher Verfahren nach Abwägung der betroffenen Interessen angemessen ist (Satz 2). Satz 3 schreibt den erforderlichen Regelungsinhalt der Verordnung vor. Satz 4 sichert die Unterrichtung des Landesbeauftragten für den Datenschutz, damit sogleich oder auch später eine datenschutzrechtliche Kontrolle durchgeführt werden kann.

Nach Absatz 3 dürfen automatisierte Abrufverfahren nur in Betrieb genommen werden, wenn vorher bestimmte organisatorische und technische Maßnahmen zur Sicherung und Kontrolle sowohl bei der übermittelnden Stelle als auch beim Empfänger getroffen sind; von besonderer Bedeutung ist dabei die in § 10 Absatz 2 Nr. 6 vorgeschriebene nachträgliche Übermittlungskontrolle.

Nach Absatz 4 gelten die Bestimmungen nach Absatz 2 Satz 2 und 3 sowie Absatz 3 entsprechend auch bei automatisierten Abrufverfahren innerhalb einer öffentlichen Stelle (interne Datenübermittlung). Der interne Datenfluß fällt zwar nicht unter den Übermittlungsbegriff des Gesetzes (vgl. § 3 Absatz 2 Satz 2 Nr. 4 und § 14 Absatz 5); um das gleichwohl auch beim internen Datenfluß vorhandene Gefährdungspotential möglichst gering zu halten, sind das Abwägungsgebot und die konkreten Festlegungen nach Absatz 2 ebenso zu beachten wie die Datensicherungsmaßnahmen nach Absatz 3.

Nach Absatz 5 sind automatisierte Abrufverfahren regelmäßig nicht zulässig im Verhältnis der öffentlichen Verwaltung zu Stellen außerhalb des öffentlichen Bereichs. Prinzipiell soll privaten Stellen kein unmittelbarer Zugriff auf Datenbanken der öffentlichen Verwaltung mit personenbezogenem Inhalt ermöglicht werden. Dies gilt nicht in den Fällen, in denen der Betroffene in Zukunft seine eigenen Daten abrufen kann.

Wenn die speichernde Stelle nach Absatz 6 die Daten veröffentlichen dürfte oder es sich um einen Anschluß an Datenbestände handelt, die jedermann ohne oder nach besonderer Zulassung offenstehen, bestehen gegen automatisierte Abrufverfahren ebenfalls keine Bedenken; in diesen Fällen kommen die Absätze 1 bis 5 nicht zur Anwendung.

Nach Absatz 7 sollen die für das automatisierte Abrufverfahren geltenden Regelungen auf die Zulassung regelmäßiger (externer und interner) Datenübermittlungen entsprechend angewandt werden. Solche Datenübermittlungen umfassen zwar nicht einen bestimmten Gesamtbestand personenbezogener Daten; gleichwohl bergen sie ein erhöhtes Gefährdungspotential in sich, weil sie geradezu „automa-

tisch", in mehr oder minder kürzeren Zeitabschnitten, dem Empfänger Daten liefern. Auch die bisherige Praxis geht davon aus, daß derartige regelmäßige Datenübermittlungen ohne ermächtigende Rechtsvorschriften nicht zulässig sind. Ein prägnantes Beispiel dafür bieten die aufgrund der Meldegesetze erlassenen Datenübermittlungsverordnungen.

Zu § 10 (Technische und organisatorische Maßnahmen)

Jede Verwendung personenbezogener Daten durch öffentliche Stellen im Rahmen der Selbst- oder der Auftragsdatenverarbeitung erfordert technische und organisatorische Maßnahmen, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten (Absatz 1 Satz 1). Datenschutz ist ohne die flankierenden Maßnahmen der Datensicherung nicht denkbar. Dabei gilt nach wie vor der Grundsatz der Zweck-Mittelrelation (Satz 2). Datensicherung gilt in Zukunft auch für die nicht formatierte (herkömmliche) Datenverarbeitung in und aus Akten. In den folgenden Absätzen werden jedoch für die automatisierte (Absatz 2) und nicht-automatisierte (Absatz 3) Datenverarbeitung differenzierte Maßnahmen vorgeschrieben; letztere umfaßt auch – anders als bisher – die nicht automatisierte dateimäßige Verarbeitung, weil sie der Datenverarbeitung in und aus Akten näher steht.

Nach wie vor erweist es sich als richtig, keine konkreten Maßnahmen, sondern nur bestimmte Sicherungsziele vorzugeben; diese sind bisher in der Anlage zu § 6 Absatz 1 Satz 1 DSG NW enthalten. Daß diese Ziele nach dem jeweiligen Stand der Technik zu realisieren sind, bedarf keiner ausdrücklichen gesetzlichen Festlegung. Auf die bisher in Absatz 2 Satz 1 enthaltene Ermächtigung der Landsregierung zur Fortschreibung der Anforderungen nach dem jeweiligen Stand der Technik und Organisation sowie auf die in den Sätzen 2 und 3 enthaltene entsprechende Definition und deren Ermittlung kann deshalb verzichtet werden. Die bisher in der Anlage zu § 6 Absatz 1 Satz 1 genannten Sicherungsziele werden wegen ihrer zunehmenden Bedeutung für die automatisierte Verarbeitung in das Gesetz selbst (Absatz 2) übernommen; dabei sind die Nrn. 2, 4, 6 und 9 gegenüber der geltenden Fassung geändert worden, um die jeweils erforderlichen Datensicherungsmaßnahmen sicherzustellen. Die übrigen bisher in der Anlage zu § 6 Absatz 1 Satz 1 enthaltenen Datensicherungsmaßnahmen haben sich in der Praxis bewährt und brauchen nicht durch schärfere Anforderungen ersetzt zu werden; sie sind aber teilweise redaktionell überarbeitet.

Absatz 3 stellt unmißverständlich klar, daß angemessene Datensicherungsmaßnahmen auch bei nicht automatisierten Dateien und Akten zu treffen sind. Gegenüber der automatisierten Datenverarbeitung sind allerdings die Gewichte der Datensicherungsmaßnahmen unterschiedlich gesetzt: Bei der nicht automatisierten Datenverarbeitung kommt der Verhinderung des Zugriffs durch Unbefugte zentrale Bedeutung zu; wird dies sichergestellt dann sind auch die unbefugte Kenntnisnahme, die Veränderung, die Löschung u.a. ausgeschlossen.

Zu § 11 (Verarbeitung personenbezogener Daten im Auftrag)

Abgesehen von verschiedenen redaktionellen Veränderungen entspricht Absatz 1 Sätze 1 und 2 inhaltlich dem bisherigen § 7 Absatz 1 Satz 1. Der Auftraggeber trägt letztlich die alleinige Verantwortung für die Einhaltung datenschutzrechtlicher Vorschriften; er ist speichernde Stelle und zugleich Adressat der Rechte des Betroffenen. Satz 3 verdeutlicht und verallgemeinert die ausschließliche Bindung des Auftragnehmers an die inhaltlichen Weisungen des Auftraggebers (vgl. bisher Absatz 2 Satz 2).

Die in den Sätzen 4 und 5 enthaltenen Regelungen gehen jedoch insofern weiter, als sie dem Auftraggeber für die Auswahl des Auftragnehmers stärkere Verpflichtungen auferlegen und bestimmen, daß die Auftragserteilung schriftlich zu erfolgen hat, wobei erforderlichenfalls zusätzliche Festlegungen zu treffen sind.

Absatz 2 enthält – wie bisher – eine Sonderregelung für die Rechenzentren des Landes, die Hochschulrechenzentren sowie die Datenverarbeitungseinrichtungen der kommunalen Gebietskörperschaften, sofern diese Zentren im Rahmen der Auftragsdatenverarbeitung für öffentliche Stellen tätig werden. Nach § 6 unterliegen die auftragnehmenden Rechenzentren unmittelbar der Wahrung des Datengeheimnisses und nach § 10 auch der Verpflichtung zur Vorhaltung technischer und organisatorischer Maßnahmen, darüber hinaus aber auch der direkten Kontrolle durch den Landesbeauftragten für den Datenschutz (§ 22 und §§ 24 bis 26). Neben die Verantwortlichkeit des Auftraggebers etwa für Maßnahmen der Datensicherung tritt die unmittelbare Verpflichtung des beauftragten Rechenzentrums; zugleich wird die direkte Kontrolle des Landesbeauftragten für den Datenschutz über den Auftragnehmer sichergestellt. Gegenüber der geltenden Fassung des § 7 Absatz 2 präzisiert der Entwurf die anzuwendenden Bestimmungen; auf den bisherigen Absatz 2 Satz 2 konnte wegen der in Absatz 1 Satz 3 vorgesehenen generellen Regelung verzichtet worden. Der neue Begriff „Kommunale Datenverarbeitungseinrichtungen" trägt

der Änderung des Gesetzes über die Organisation der automatisierten Datenverarbeitung in Nordrhein-Westfalen – ADVG NW – vom 21. 12. 1984 (GV. NW. S. 750) Rechnung.

Die in Absatz 3 vorgesehene Regelung entspricht im Grundsatz dem bisherigen § 7 Abs. 1 Satz 2. Sie macht jedoch aus Gründen der Rechtsklarheit deutlich, daß es eine Kontrollkompetenz des Landesbeauftragten für den Datenschutz nach den Maßstäben des Landesdatenschutzgesetzes nur innerhalb des Landes Nordrhein-Westfalen geben kann. Eine Ausdehnung nordrhein-westfälischer Kontrollmaßstäbe und Kontrollkompetenzen auf nicht-öffentliche Stellen des Privatrechts in anderen Bundesländern wirft eine Reihe schwerwiegender Rechtsfragen auf, die nur durch einen entsprechenden Staatsvertrag gelöst werden könnten; bisher hat die Praxis die Notwendigkeit für eine solche länderübergreifende Regelung nicht ergeben. Die vorgesehene Beschränkung auf den Landesbereich führt auch zu keiner unvertretbaren Kontrollücke: Verarbeitet eine private Stelle im Auftrag einer öffentlichen Stelle personenbezogene Daten, unterliegt sie den Kontrollmechanismen des Bundesdatenschutzgesetzes, insbesondere der Kontrolle der zuständigen Aufsichtsbehörde. Um in diesen Fällen eine effektive Kontrolle sicherzustellen, soll die öffentliche Stelle, in deren Auftrag die Datenverarbeitung erfolgt, die jeweils zuständige Datenschutzkontrollbehörde über die Auftragsdatenverarbeitung unterrichten.

Zu § 12 (Erhebung)

Mit der Veränderung der Überschrift des bisherigen § 10 sowie der weitgehenden Neufassung dieser Vorschrift wird das „Erheben" oder die „Erhebung" personenbezogener Daten (in der Definition des § 3 Abs. 2 Satz 2 Nr. 1) als neue Datenverarbeitungsphase in das Gesetz eingeführt.

Prinzipielle Voraussetzung jeder Erhebung ist, daß sich die Beschaffung personenbezogener Daten aus der jeweiligen Aufgabenzuweisungsnorm der datenverarbeitenden Stelle als erforderlich erweist (Absatz 1 Satz 1).

Ist in diesem Sinne die Kenntnis bestimmter personenbezogener Daten zur rechtmäßigen Aufgabenerfüllung der öffentlichen Stelle erforderlich, folgt die Entscheidung über die Art der Datenverarbeitung und ihre Form.

Nach dem neuen Satz 2 darf eine an sich zulässige Datenerhebung nur in einer Art und Weise durchgeführt werden, die das allgemeine Persönlichkeitsrecht des Betroffenen nicht beeinträchtigt. Damit sollen unangemessene und unzumutbare Methoden bei der Erhebung, ebenso aber auch unzumutbare Fragen ausgeschlossen werden.

Satz 3, 1. Halbsatz, enthält das Postulat, daß – im Sinne des Rechts auf informationelle Selbstbestimmung – die Verwaltungsbehörden die von ihnen benötigten personenbezogenen Daten grundsätzlich unmittelbar beim Betroffenen mit seiner Kenntnis zu erheben haben. Denn nur auf diesem Wege kann er sein Recht, selbst über die Preisgabe und Verwendung seiner Daten bestimmen zu dürfen, wirksam ausüben. Die Erhebung personenbezogener Daten ohne seine Kenntnis – bei Behörden oder privaten Stellen – oder auch durch heimliche Observation soll generell ausgeschlossen ein. Auf einige – eng umgrenzte – Ausnahmetatbestände kann allerdings nicht vollständig verzichtet werden, weil in einer Reihe von Fällen aus überwiegendem öffentlichem oder besonderem privatem Interesse eine Beschaffung personenbezogener Daten auch ohne Kenntnis des Betroffenen möglich sein muß. Eine solche Beschaffung bei einer anderen Stelle ist der Situation vergleichbar, in der eine Behörde ursprünglich zu bestimmten Zwecken erhobene Daten ohne Wissen des Betroffenen zu anderen Zwecken verarbeitet. Die Erhebung personenbezogener Daten ohne Kenntnis des Betroffenen ist daher nach Satz 3, 2. Halbsatz, nur unter den gleichen Voraussetzungen zulässig, unter denen § 13 Absatz 2 Satz 1 Buchst. a bis h die nachträgliche Zweckänderung erhobener Daten legitimiert.

Wegen der danach im einzelnen in Betracht kommenden Fälle wird auf die Begründung zu § 13 (Zweckbindung bei Speicherung, Veränderung und Nutzung) verwiesen.

Nicht unter den Erhebungsbegriff fallen personenbezogene Daten, die vom Betroffenen selbst oder von Dritten **ohne** Anforderung der öffentlichen Stelle geliefert werden sowie Erkenntnisse, die der Verwaltungsbehörde **durch Zufall** bekannt werden. Aber auch in diesen Fällen ist nur eine eingeschränkte Verwertbarkeit im Rahmen rechtmäßiger Aufgabenerfüllung vorgesehen (vgl. zu § 13 Absatz 1 Satz 1 i.V.m. Satz 3).

Absatz 2, der die Verpflichtungen gegenüber dem Betroffenen regelt, entspricht im Grundsatz dem bisherigen § 10 Absatz 2 Satz 1. Die Vorschrift gewinnt mit der Einführung der Erhebung wesentlich größere Bedeutung. Erhebungen mit oder ohne Auskunftsverpflichtung des Betroffenen werden deutlicher voneinander unterschieden; die jeweils zu beachtenden Hinweis- und Aufklärungspflichten der erhebenden

Stelle werden präzisiert und verstärkt. Die bisherige Regelung in Absatz 2 Satz 2 ist im neuen Satz 3 mitenthalten (vgl. auch Zu § 4 Satz 4).

Absatz 3 betrifft die Erhebung bei Dritten oder nicht-öffentlichen Stellen; nähere Auskünfte über den Verwendungszweck sollen nur auf Verlangen gegeben werden. Obligatorisch ist aber die Belehrung über die jeweilige Rechtsgrundlage der Erhebung.

Zu § 13 (Zweckbindung bei Speicherung, Veränderung und Nutzung)

Der neue § 13 stellt das Kernstück der vorgesehenen Neukonzeption datenschutzrechtlicher Regelungen dar. Die Vorschrift soll die verfassungsrechtlich gebotene Zweckidentität zwischen der Erhebung bzw. Verarbeitung ohne Erhebung und der weiteren Verwendung personenbezogener Daten sicherstellen; zugleich regelt sie die zulässigen Ausnahmen vom Zweckbindungsgebot. Für die Übermittlungsphase gelten dabei die §§ 14–17.

Absatz 1 Satz 1 enthält die zentrale Zweckbindungsregelung für die Datenverarbeitung durch eine öffentliche Stelle, die beim Bürger personenbezogene Daten zu bestimmten Zwecken zulässigerweise erhoben hat. Das mit der Einführung der Erhebungsphase gewährleistete Recht des Betroffenen, im Regelfall selbst über die Preisgabe und Verwendung seiner Daten bestimmen zu dürfen, hat zur logischen Konsequenz, daß der Verwendungszweck der Daten bei der anschließenden Verarbeitung grundsätzlich nicht ohne Wissen des Betroffenen geändert werden darf (Absatz 1 Satz 2).

Die Zweckbindung gilt aber nicht nur für personenbezogene Daten, die zielgerichtet erhoben worden sind, sondern auch für solche Informationen, die der Verwaltung ohne ihr Zutun zugehen (Absatz 1 Satz 3). Werden diese Daten zulässigerweise im Rahmen der rechtmäßigen Aufgabenerfüllung entsprechend Absatz 1 Satz 1 gespeichert, dann setzt mit diesem zielgerichteten Handeln die Zweckbindung ein.

Nach Absatz 2 Satz 1 ist bei beiden Fallgruppen die mit einer Zweckänderung verbundene Verarbeitung personenbezogener Daten nur bei Vorliegen besonderer eng begrenzter Ausnahmetatbestände zulässig. Die zulässigen Ausnahmen von Zweckbindungsgebot sind in den Buchstaben a bis i alternativ aufgezählt.

Zulässig ist danach gemäß Buchstabe a eine Zweckänderung zunächst in denjenigen Fällen, in denen eine Rechtsvorschrift dies ausdrücklich erlaubt; ferner in den Fällen, in denen die Wahrnehmung einer durch Gesetz oder Rechtsverordnung der Behörde zugewiesenen Aufgabe die Verarbeitung ganz bestimmter personenbezogener Daten zwingend voraussetzt. Die Vorschrift soll der öffentlichen Stelle nicht prinzipiell die Möglichkeit einräumen, etwa ohne bereichsspezifische Normen Datenverarbeitung betreiben zu dürfen, sondern sie nur in denjenigen Fällen zur Datenverarbeitung legitimieren, in denen der Zweck vorhandener Normen eine andere Interpretation ausschließt.

Zulässig ist eine Zweckänderung nach Buchstabe b ferner in denjenigen Fällen, in denen der Betroffene z.B. bei Stellung eines Antrags zum Ausdruck gebracht hat, daß die Behörde bestimmte Ermittlungen anstellen darf (vgl. insoweit § 4 im besonderen Satz 4).

Dies gilt insbesondere bei der Benutzung behördlicher Vordrucke, die so zu gestalten sind, daß der Betroffene erfährt, wo Daten über ihn erhoben werden können, und ggf. von der Stellung des Antrags absehen kann, wenn ihm die erforderlichen Abfragen unerwünscht sind.

Auch ohne Einwilligung des Betroffenen dürfen nach Buchstabe c personenbezogene Daten, die zu anderem Zweck gespeichert sind, von der Behörde zur Überprüfung von Angaben des Betroffenen verwendet werden, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Angaben unrichtig sind. In diesen Fällen wird dem Grundsatz rechtmäßiger Aufgabenerfüllung Priorität zuerkannt. Dies liegt auch im Interesse des Betroffenen, der sich sonst möglicherweise später Regreßansprüchen oder sonstigen Maßnahmen der öffentlichen Verwaltung ausgesetzt sieht.

Eine Aufhebung der Zweckbindung ist nach Buchstabe d grundsätzlich zulässig, wenn es gilt, erhebliche Nachteile für das Gemeinwohl abzuwehren; entsprechendes gilt für die Abwehr einer sonst unmittelbar drohenden Gefahren für die öffentliche Sicherheit. In der Regel wird hierbei allerdings als Rechtsgrundlage eine bereichsspezifische Bestimmung vorrangig eingreifen. Andererseits können sich aus bereichsspezifischen – abschließenden – Regelungen, z. B. dem SGB X, insoweit auch gewisse Einschränkungen ergeben.

Mit der Regelung in Buchstabe e soll die anderweitige Nutzung bereits bei der öffentlichen Stelle vorhandener personenbezogener Daten in solchen Fällen ermöglicht werden, in denen die Verwendung der personenbezogenen Daten nach pflichtgemäßer Prüfung offensichtlich im Interesse des Betroffenen liegt,

Nachteile für diesen nicht zu befürchten sind und deshalb davon ausgegangen werden kann, daß dieser seine Einwilligung zur Zweckänderung erteilen würde (sog. Bürgerservice).

Eine Zweckänderung gespeicherer Daten ist auch in denjenigen Fällen zulässig (Buchstabe f), in denen die Daten von der öffentlichen Stelle unmittelbar aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte. Da die in Betracht kommenden Daten bereits in der Öffentlichkeit verfügbar sind oder publiziert werden dürfen, bestehen keine Bedenken, wenn unter diesen Voraussetzungen eine Zweckänderung zugelassen wird; gleichwohl ist dies in denjenigen Fällen unzulässig, in denen das Geheimhaltungsinteresse des Betroffenen einer solchen Verwendung der Daten offensichtlich entgegensteht.

Buchstabe g überträgt die in Buchstabe d zugunsten der Gemeinschaft vorgesehene Ausnahmeregelung auf den Schutz der Rechte einer anderen Person. Werden deren Rechte schwerwiegend gefährdet (z. B. Leib, Leben, Freiheit, aber auch wesentliche Vermögensinteressen), muß das Recht des Betroffenen auf Wahrung des informationellen Selbstbestimmungsrechts zurücktreten. Eine Zweckänderung gegenüber personenbezogenen Daten ist auch zulässig im Rahmen der Verleihung von Orden und Ehrenzeichen (Buchst. h), soweit nicht bereichsspezifische Regelungen bestehen.

Buchstabe i sieht ferner Durchbrechungen der Zweckbindung vor, die die Verfolgung von Straftaten oder Ordnungswidrigkeiten, die Strafvollstreckung und den Strafvollzug und weitere gerichtliche Maßnahmen ermöglichen sollen. Für die Organe der Rechtspflege bleiben insoweit allein die besonderen gesetzlichen Verfahrensvorschriften (z. B. der StPO) maßgeblich.

Nach Absatz 2 Satz 2 kommt eine Zweckänderung bei amtlich übermittelten personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, wegen ihrer besonderen Sensitivität ohne Rechtsnorm oder Einwilligung des Betroffenen nicht in Betracht.

Absatz 3 stellt klar, daß die Nutzung personenbezogener Daten im Rahmen von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder auch von Organisationsuntersuchungen nicht als Zweckänderung anzusehen ist. Zulässig ist auch grundsätzlich die Verarbeitung personenbezogener Daten im Rahmen von Ausbildungs- und Prüfungszwecken, zumal in diesen Fällen ein eigentliches Interesse an dem Personenbezug der Daten nicht besteht.

Zu § 14 (Übermittlung innerhalb des öffentlichen Bereichs)

Nach der bisherigen Fassung des § 11 Abs. 1 Satz 1 ist die Übermittlung personenbezogener Daten von einer öffentlichen Stelle an eine andere schon immer dann zulässig, wenn sie entweder zur rechtmäßigen Erfüllung einer eigenen oder auch einer fremden Aufgabe erforderlich ist; im letzteren Fall wird die speichernde Stelle in der Regel von einer anderen öffentlichen Stelle im Wege der Amtshilfe um Auskunft (Informationshilfe) ersucht. Diese Gleichstellung von eigener und fremder Aufgabenerfüllung, die an keine besonderen Zulässigkeitskriterien gebunden ist, kann nicht unverändert beibehalten werden, weil sie dem verfassungsrechtlichen Anliegen einer grundsätzlich zweckgebundenen Datenerhebung und Datenverarbeitung nicht entspricht. Die Übermittlungsregelungen dieses Gesetzes orientieren sich dagegen – dies gilt insbesondere für den Nachrichtenaustausch von Behörden – prinzipiell am Grundrecht auf informationelle Selbstbestimmung. Soweit nicht bereichsspezifische gesetzliche Vorschriften etwas anderes bestimmen, ist eine gegenseitige Informationshilfe öffentlicher Stellen unter Durchbrechung der Zweckbindung nur noch unter den in dieser Vorschrift aufgeführten Voraussetzungen zulässig. § 14 ist zugleich als spezielle und damit vorrangige landesrechtliche Rechtsvorschrift im Sinne des § 1 Abs. 1 des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen (VwVfG NW) für die Übermittlung **personenbezogener** Daten auf Ersuchen einer anderen öffentlichen Stelle anzusehen (vgl. hierzu Artikel 3 – Änderung des Verwaltungsverfahrensgesetzes für das Land NRW –, § 3a).

Die bisher in § 11 Absatz 1 Satz 2 geregelte Übermittlung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, kann im Hinblick auf die Intensität des möglichen Eingriffs nicht mehr Gegenstand einer Regelung des allgemeinen Datenschutzrechts sein. Ob und inwieweit Übermittlungen solcher personenbezogener Daten zulässig sind, ist nur bereichsspezifisch zu regeln.

Die bisherigen Regelungen des § 11 Abs. 2 sind in § 15 (neu) enthalten.

Im einzelnen gilt folgendes:

Wie bisher setzt Absatz 1 Satz 1 zunächst voraus, daß die Datenübermittlung im Rahmen der Aufgabenerledigung der übermittelnden Stelle oder des Empfängers erforderlich ist. Darüber hinaus müssen jedoch für die Übermittlung weitere Zulässigkeitsvoraussetzungen gegeben sein: Für die übermittelnde Stelle gilt zunächst, daß die Datenübermittlung zulässig ist, wenn Zweckidentität zwischen der Erhe-

bung/Speicherung und der weiteren Verwendung gemäß § 13 Absatz 1 Satz 2 oder Satz 3 besteht, die Daten also jedenfalls auch zum Zwecke der Übermittlung erhoben bzw. gespeichert wurden. Liegen diese Voraussetzungen nicht vor, so ist gleichwohl eine Datenübermittlung zugunsten des Empfängers zulässig, wenn die Zweckänderung nach den Ausnahmevorschriften des § 13 Abs. 2 Satz 1 Buchst. a bis i legitimiert ist. Für den Betroffenen macht es nämlich keinen prinzipiellen Unterschied, ob eine öffentliche Stelle erhobene Daten zu anderen Zwecken selbst verarbeitet oder ob die Zweckänderung in der Weise geschieht, daß diese Daten an eine andere öffentliche Stelle zur rechtmäßigen Aufgabenerfüllung übermittelt werden.

Satz 1 letzter Halbsatz stellt klar, daß eine Übermittlung zur Wahrnehmung von Aufgaben nach § 13 Abs. 3 (Aufsichts- und Kontrollbefugnisse) immer zulässig ist.

Die in Absatz 1 Satz 2 vorgesehene Regelung entspricht den Erfordernissen komplexer Verwaltungsverfahren, bei denen mehrere öffentliche Stellen an einem Entscheidungsprozeß beteiligt sind. Dies gilt entsprechend beim Zusammenwirken mehrerer datenverarbeitender Stellen innerhalb der Organisationseinheit einer Behörde (vgl. Absatz 5).

Absatz 2 trägt den Besonderheiten bei der Übermittlung personenbezogener Daten in und aus Akten Rechnung. Während sich bei automatisierter Datenverarbeitung in der Regel diejenigen Daten aussondern lassen, die zur jeweiligen Aufgabenerfüllung nicht erforderlich sind und deshalb nicht übermittelt werden dürfen, ist eine solche Trennung bei Akten nicht ohne weiteres möglich. Stattdessen muß eine Vielzahl aktuell nicht relevanter personenbezogener Daten während der Bearbeitung zur Kenntnis genommen, übermittelt oder innerhalb der datenverarbeitenden Stelle weitergegeben werden, weil diese untrennbar mit Daten verbunden sind, deren Verarbeitung für die jeweilige Aufgabenerfüllung erforderlich ist. Diese Problematik ist von besonderer Bedeutung bei der Übermittlungsphase. Soweit daher nicht berechtigte Interessen des Betroffenen oder eines Dritten an der Geheimhaltung der für die Bearbeitung nicht erforderlichen Daten offensichtlich überwiegen, soll die Übermittlung vollständiger Aktenunterlagen zulässig sein; bezüglich der nicht zur Aufgabenerfüllung erforderlichen personenbezogenen Daten gilt allerdings ein Verwertungsverbot.

Absatz 3 regelt die Verantwortlichkeit für die datenschutzrechtliche Zulässigkeit von Datenflüssen zwischen öffentlichen Stellen. Eine solche Regelung fehlt bisher im geltenden Recht.

Nach Satz 1 trägt grundsätzlich die übermittelnde Stelle die Verantwortung für die Übermittlung personenbezogener Daten. Der übermittelnden Stelle kann in der Regel aber keine Verantwortung für eine Entscheidung aufgebürdet werden, deren Notwendigkeit und Auswirkungen sie nicht beurteilen kann. Sie hat daher im Ersuchensfall nur die Plausibilität des Übermittlungsersuchens zu prüfen (Satz 2). Sie muß aber die Zulässigkeit der Übermittlung prüfen, wenn sie im Einzelfall Anhaltspunkte besitzt, an der Rechtmäßigkeit des Ersuchens zu zweifeln. In diesem Fall besteht für den Empfänger eine besondere Informationsverpflichtung (Satz 3).

Bei Übermittlungen im Rahmen automatisierter Abrufverfahren (§ 9), bei denen die abrufende Stelle über den Bestand der speichernden Stelle verfügen kann, trägt diese die (alleinige) Verantwortung für die Rechtmäßigkeit des Abrufs (Satz 4).

Nach Absatz 4 gilt auch bei zulässiger Übermittlung personenbezogener Daten für den Empfänger das Zweckbindungsgebot. Ausnahmen hiervon sind nur unter den engen Voraussetzungen des § 13 Absatz 2 zulässig.

Nach Absatz 5 sollen die für die Übermittlung geltenden Bestimmungen der Absätze 1 bis 4 auch beim Datenfluß innerhalb einer öffentlichen Organisationseinheit entsprechende Anwendung finden. Die besondere Bestimmung ist erforderlich, weil eine solche Datenweitergabe keine Übermittlung an Dritte nach § 3 Abs. 2 Satz 2 Nr. 4 darstellt. Gleichwohl kann es nicht angehen, die Datenweitergabe innerhalb einer öffentlichen Stelle unbeschränkt zuzulassen; auch sie muß am Grundrecht des informationellen Selbstbestimmungsrechts gemessen werden.

Für eine solche Beschränkung sprechen im übrigen bereits der Grundgedanke des § 8 Satz 1 des geltenden Rechts und verschiedene bereichsspezifische Regelungen (vgl. SGB X), die – ausgehend vom funktionellen Behördenbegriff – einen unbeschränkten Datenaustausch auch innerhalb einer öffentlichen Stelle nicht zulassen.

Zu § 15 (Übermittlung an öffentlich-rechtliche Religionsgesellschaften)

§ 15 entspricht im Wortlaut weitgehend dem bisherigen § 11 Absatz 2. Bei der Anwendung dieser Vorschrift ist künftig aber der § 14 i.V.m. § 13 zu berücksichtigen. Überwiegend erfolgt bisher die Datenübermittlung aufgrund bereichsspezifischer Normen (vgl. § 32 Meldegesetz NW).

Zu § 16 (Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs)

Absatz 1 (bisher § 13 Absatz 1) ist redaktionell neu gefaßt und zugleich inhaltlich wesentlich verändert. Der bisherige Absatz 1 Satz 1, der die Übermittlungsvoraussetzungen enthält, soll wesentlich differenzierter gestaltet werden. Der neue Absatz 1 Satz 1 Buchst. a bis d und Satz 2 stellen auf die jeweils unterschiedliche Interessenlage von Verwaltung und Dritten bei der Übermittlung personenbezogener Daten an Personen und Stellen außerhalb des öffentlichen Bereichs ab.

In Absatz 1 Satz 1 Buchst. a wird eine Übermittlung – entsprechend der Regelung in § 14 Absatz 1 Satz 1 (1. Alternative) – an die Erforderlichkeit und an das Zweckbindungsgebot in § 13 Absatz 1 gebunden.

In Absatz 1 Satz 1 Buchst. b ist geregelt, daß solche Datenübermittlungen auch dann zulässig sind, wenn die Voraussetzungen des § 13 Absatz 2 Satz 1 Buchst. a, b, d, f oder g erfüllt sind, weil hier das informationelle Selbstbestimmungsrecht zurückzutreten hat oder nur unwesentlich tangiert wird.

Absatz 1 Satz 1 Buchst. c und d regeln zwei unterschiedliche Fälle, in denen personenbezogene Daten aus dem öffentlichen Bereich übermittelt werden. Bisher genügt dafür nach § 13 Abs. 1 Satz 1 das Glaubhaftmachen eines berechtigten Interesses; allerdings dürften dabei schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Würde man an diesen Voraussetzungen unverändert festhalten, wäre an einen Dritten die Übermittlung personenbezogener Daten aus dem öffentlichen Bereich unter leichteren Bedingungen möglich als der Datenaustausch zwischen verschiedenen öffentlichen Stellen. Daten der öffentlichen Verwaltung dienen aber in erster Linie der Erfüllung öffentlicher Aufgaben; nur unter besonderen Voraussetzungen stehen sie für die Interessen privater Dritter zur Verfügung.

Nach Satz 1 Buchst. c ist eine Übermittlung immer dann zulässig, wenn ein **rechtliches** Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und kein Grund zu der Annahme besteht, daß das Geheimhaltungsinteresse des Betroffenen überwiegt. Eine Übermittlung soll daher unter erleichterten Voraussetzungen auch dann nach Satz 1 Buchst. d, 2. Alternative zulässig sein, wenn hierfür ein berechtigtes Interesse geltend gemacht wird und der Betroffene nach entsprechender Information durch die Behörde (Satz 2) der beabsichtigten Datenübermitlung nicht widersprochen hat. Dies gilt unter den gleichen Voraussetzungen, wenn die Übermittlung im öffentlichen Interesse liegt (Satz 1 Buchst. d, 1. Alternative).

Bereichsspezifische Sonderregelungen (z.B. für Auskünfte aus öffentlichen Registern) bleiben unberührt.

Aus den bereits zu § 14 ausgeführten Gründen ist in Absatz 1 keine allgemeine Regelung über die Zulässigkeit der Übermittlung personenbezogener Daten aus Berufs- oder besonderen Amtsgeheimnissen mehr vorgesehen. Die Bedeutung der bisherigen Regelung (Absatz 1 Satz 2) erscheint ohnehin fraglich; sie kann auch angesichts der Sensitivität der infrage kommenden Daten nicht aufrechterhalten bleiben. Die Übermittlungsvoraussetzungen müssen künftig im Rahmen bereichsspezifischer Regelungen bestimmt werden.

Die bisher in § 13 Abs. 1 Satz 3 enthaltenen Regelungen für die Übermittlung an Behörden oder Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen sind in einer selbständigen Vorschrift enthalten (vgl. § 17).

Die in Absatz 2 bestimmte weitere Zweckbindung übermittelter Daten entspricht inhaltlich dem bisherigen Recht (§ 13 Abs. 2).

Zu § 17 (Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes und zur Aufhebung der bisherigen §§ 14 und 15)

Nach Satz 1 ist die Übermittlung personenbezogener Daten an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen zulässig, soweit dies in einem Gesetz oder einer internationalen Vereinbarung ausdrücklich geregelt ist. Der Vorschrift kommt damit im Hinblick auf die angesprochenen Sonderregelungen keine eigenständige konstitutive Bedeutung zu. Im Ergebnis besteht eine inhaltliche Übereinstimmung mit der bisher in § 13 Abs. 1 Satz 3 getroffenen Regelung.

Demgegenüber enthält Satz 2 eine eigenständige Übermittlungsregelung, die in erster Linie für die Übermittlung im Einzelfall in Betracht kommt. Die Übermittlung personenbezogener Daten an ausländische oder über- und zwischenstaatliche Stellen (insbesondere im Bereich der Europäischen Wirtschaftsgemeinschaft) soll unter den gleichen Voraussetzungen zulässig sein wie der Informationsaustausch zwischen Stellen innerhalb des öffentlichen Bereichs. Erforderlich ist dazu, daß die Voraussetzungen des § 14 Absatz 1 Satz 1 erfüllt sind und äquivalente Datenschutzregelungen im Empfängerland bestehen.

Eine Vorbehaltsklausel stellt sicher, daß die Übermittlung dennoch in Fällen unterbleiben muß, in denen Grund zu der Annahme besteht, daß dadurch gegen das informationelle Selbstbestimmungsrecht oder den Zweck eines anderen Gesetzes im Geltungsbereich des Grundgesetzes verstoßen würde (Vorbehalt des ordre public).

Die bisherigen §§ 14 und 15 (Rechtsverordnung zur Datenübermittlung und Veröffentlichung über die gespeicherten Daten) **werden ersatzlos aufgehoben.**

Es bestehen schon Zweifel, ob die Ermächtigung in § 14 angesichts der Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsurteil noch Bestand haben kann; zum anderen hat die Praxis der vergangenen Jahre gezeigt, daß bisher von dieser Rechtsverordnungsermächtigung kein Gebrauch gemacht worden ist. Die nach dieser Vorschrift beabsichtigten Detailregelungen für bestimmte Sachbereiche können nicht generell, sondern nur im Rahmen bereichsspezifischer gesetzlicher Lösungen getroffen werden. Ein typisches Beispiel dafür sind die Regelungen des Meldegesetzes und der danach erlassenen Datenübermittlungsvorschriften.

Auch § 15 hat sich in der Praxis nicht bewährt. Das bisherige Nebeneinander der Veröffentlichung bzw. Registrierung nach § 15 und § 27 ist mit erheblichem Verwaltungsaufwand verbunden. Der Zweck dieser Vorschrift kann durch die vorgesehene Dateibeschreibung (§ 8), die darauf abgestimmte Neuregelung des Dateienregisters (§ 23) und durch die erweiterten Auskunfts- und Einsichtsrechte im Einzelfall (§ 18) gleich wirksam, dabei aber mit geringerem bürokratischen Aufwand gesichert werden.

Zu § 18 (Auskunft, Einsicht in Akten)

Der Auskunftsanspruch des Betroffenen gehört zu den wesentlichen Datenschutzrechten des Bürgers. Um die Bedeutung dieser Rechte angemessen hervorzuheben, sieht der Entwurf einen eigenen (dritten) Abschnitt für die Rechte des Betroffenen vor. Die neue – differenziert gestaltete – Vorschrift über das Auskunfts- bzw. Einsichtsrecht hat sich zum Ziel gesetzt, die Rechtsstellung des Betroffenen zu verbessern. Mehr Transparenz im Rahmen der Datenverarbeitung soll dazu beitragen, die geeigneten Voraussetzungen zu schaffen, daß der Betroffene seine sonstigen Rechte auf Grund dieses Gesetzes wirksam geltend machen kann. Dazu gehört auch, daß er die ihn betreffenden Informationen unentgeltlich erhält.

Zunächst wird, unabhängig davon, ob es sich um eine dateimäßige oder nicht dateimäßige Datenverarbeitung handelt, in Absatz 1 Satz 1 die Auskunftspflicht um Angaben erweitert, die bisher bereits teilweise Gegenstand der Veröffentlichung nach § 15 a. F. waren. Künftig soll sich das Auskunftsrecht über die zur Person in Dateien gespeicherten Daten und Empfänger regelmäßiger Übermittlungen hinaus auf den Zweck und die Rechtsgrundlage der Speicherung (so bisher § 16 Absatz 1 Satz 1) sowie die Herkunft der Daten und die Empfänger aller Übermittlungen erstrecken.

Da der Auskunftsanspruch sowohl bei dateimäßiger als auch bei nicht dateimäßiger Datenverarbeitung besteht, kommt es in Zukunft nicht darauf an, ob die jeweiligen Angaben ganz oder nur teilweise dateimäßig gespeichert sind. Auf die bisher in § 16 Absatz 1 Satz 2 enthaltene Regelung über die Mitwirkung des Antragstellers kann als Selbstverständlichkeit verzichtet werden; in der Regel wird jede summarische Angabe gegenüber der speichernden Stelle genügen, um den Anspruch auszulösen. Die bisherige Verfahrensregelung nach Satz 3 findet sich in Absatz 2 Satz 1, 1. Halbsatz.

Absatz 1 Satz 2 enthält die Ausnahmen von der Auskunftspflicht; sie **erstrecken** sich auf ausschließlich zum Zwecke der Datensicherung oder der Datenschutzkontrolle gespeicherte Daten und auf gesperrte, nicht mehr benötigte Daten, die auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen (bisher § 16 Absatz 2 i. V. m. § 15 Absatz 2 Nr. 2). In diesen Fällen ist eine Auskunftspflicht entbehrlich, da die Daten ohne sonderliches Interesse für den Betroffenen sind und auch nicht mehr weiterverarbeitet werden dürfen.

Wie bisher bestimmt die Behörde die Form der Auskunftserteilung nach pflichtgemäßem Ermessen (Absatz 2 Satz 1, 1. Halbsatz). Für personenbezogene Daten in **Akten** sieht Satz 1, 2. Halbsatz eine zusätzliche Regelung vor; sie will der Tatsache gerecht werden, daß Akten im Einzelfall schwerer zu finden und auszuwerten sind als Dateien. Zwar richtet sich auch für Akten das Auskunftsrecht nach den Voraussetzungen des Absatzes 1; wahlweise kann der Betroffene jedoch statt oder neben der Auskunft Akteneinsicht verlangen. Die Alternativregelung greift damit Überlegungen auf, dem Bürger ein möglichst weites Informationsrecht an seinen eigenen Daten gegenüber der öffentlichen Verwaltung einzuräumen. Die Akteneinsicht kann auch für die Behörde günstiger sein, wenn etwa umfangreiche Akten durchsucht werden müßten, ob und welche Daten über die anfragende Person darin enthalten sind.

Das Auskunfts- und Einsichtsverfahren ist allerdings bei Akten aus Gründen der Verwaltungspraktikabilität (Auffindbarkeit) an qualifizierte Voraussetzungen gebunden (Absatz 2 Satz 2). Der Betroffene muß wegen des sachnotwendig größeren Verwaltungsaufwandes bei Auskunftsbegehren aus Akten jedenfalls so konkrete Angaben machen, daß die Daten aufgefunden werden können; der zu listende Aufwand darf dabei nicht außer Verhältnis zu dem nicht näher begründeten oder dem im Einzelfall dargelegten Informationsinteresse stehen.

Die Regelung des § 18 DSG NW über die Akteneinsicht findet keine Anwendung, soweit das Akteneinsichtsrecht und die Modalitäten der Einsichtsgewährung erkennbar abschließend in bereichsspezifischen Gesetzen (beispielsweise in der StPO) geregelt sind (vgl. § 2 Absatz 3 DSG NW neu). In § 18 Absatz 2 Satz 2 wird klargestellt, daß auch die Regelung des Verwaltungsverfahrensgesetzes über die Akteneinsicht durch Verfahrensbeteiligte (§ 29 VwVfG NW) das Akteneinsichtsrecht nach § 18 DSG NW verdrängt, soweit die in § 29 VwVfG NW genannten Voraussetzungen vorliegen.

Nach Absatz 3 ist die Verpflichtung öffentlicher Stellen zur Erteilung von Auskunft und Einsicht generell anders strukturiert: Die bisherige Regelung, wonach bestimmte Behörden (Verfassungsschutz, Staatsanwaltschaft und Polizei sowie Landesfinanzbehörden) von der Verpflichtung zur Auskunft gänzlich ausgenommen sind (§ 16 Absatz 2 i.V.m. § 15 Absatz 2 Nr. 1), ist mit dem Recht auf informationelle Selbstbestimmung unvereinbar und kann daher nicht mehr aufrechterhalten werden. Grundsätzlich muß jeder erfahren dürfen, wer was wann und bei welcher Gelegenheit über ihn gespeichert hat. Ausnahmen von diesem Grundsatz sind nur zulässig, wenn die Einzelabwägung ergibt, daß überwiegende Gründe des Gemeinwohls der Auskunftserteilung entgegenstehen. Die Tatbestände in den Buchst. a bis c enthalten solche Beschränkungen des Auskunftsrechts, die der Auskunftsersuchende im Gemeinwohlinteresse zu akzeptieren hat. Im Hinblick auf die für die Zukunft angestrebte einheitliche Handhabung durch die öffentliche Verwaltung sind die Ausnahmetatbestände an die Regelung des § 29 Absatz 2 VwVfG NW angeglichen. Bei der Beurteilung der Tragweite dieser Regelung ist allerdings zu berücksichtigen, daß die Abfrage eigener personenbezogener Daten bei Behörden außerhalb des Sicherheitsbereichs nicht ohne weiteres zu einer Beeinträchtigung bzw. Gefährdung im Sinne des Absatz 3 Nrn. 1 und 2 führen kann. Im Rahmen der Nr. 3 können besondere Rechtsvorschriften bzw. berechtigte Interessen von Dritten an der Geheimhaltung zusätzlich eine Auskunftsverweigerung begründen.

Nach Absatz 4 bedarf die Auskunftsverweigerung grundsätzlich einer Begründung. Wird die Auskunft zu Recht verweigert und ist eine Offenlegung der Gründe gegenüber dem Betroffenen nicht möglich, so sind die wesentlichen Gründe für diese Entscheidung in einer Weise zu dokumentieren, die eine Nachprüfung durch die zuständigen Stellen – in der Regel durch den Landesbeauftragten für den Datenschutz – ermöglicht.

Eine Sonderregelung enthält Absatz 5: Danach sind Auskunftserteilung und Akteneinsichtsgewährung durch öffentliche Stellen über die Herkunft personenbezogener Daten von den Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, unter bestimmten Voraussetzungen von den Landesfinanzbehörden sowie von den im bisherigen § 12 Abs. 2 Nr. 1 BDSG aufgeführten Dienststellen des Bundes im Sicherheitsbereich nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Damit wird bei prinzipieller Anerkennung des Auskunftsrechts der Notwendigkeit Rechnung getragen, daß über solche Auskunftsbegehren letztlich nur die in der Sache betroffenen Stellen entscheiden können; bei der Versagung der Zustimmung gelten aber die Absätze 3 und 4 entsprechend, soweit es sich um Landesbehörden handelt.

Wird aus den vorgenannten Gründen Auskunft oder Akteneinsicht nicht gewährt, so ist die öffentliche Stelle nach Absatz 6 verpflichtet, den Betroffenen darauf hinzuweisen, daß er sich in dieser Angelegenheit an den Landesbeauftragten für den Datenschutz wenden kann, um auf diese Weise unter Umständen eine (unverzügliche) Nachprüfung der Auskunftsverweigerung zu erreichen.

Zu § 19 (Berichtigung, Sperrung und Löschung)

Die neugefaßte Vorschrift verbessert die Rechtsposition des Betroffenen bei den Korrekturansprüchen. Von besonderer Bedeutung ist die Einführung der obligatorischen Löschungsverpflichtung für die datenverarbeitenden öffentlichen Stellen in den Fällen, in denen die Kenntnis der Daten für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist. Diese Regelung kann den ihr zugedachten Zweck jedoch nur erfüllen, wenn flankierend entsprechende archivrechtliche Vorschriften existieren. Darüber hinaus enthält die Vorschrift notwendige Sonderregelungen für die Berichtigung, Sperrung und Löschung personenbezogener Daten in Akten. Wegen der Übergangsregelung für Akten wird auf § 35 verwiesen.

Im einzelnen gilt folgendes:

Absatz 1 Satz 1 ist unverändert. Satz 2 modifiziert das Berichtigungsverfahren in nicht-automatisierten Dateien oder Akten. Aus Praktikabilitätsgründen wird die Art und Weise der Berichtigung im Gesetz nicht vorgeschrieben. Bei Akten soll sie in der Weise gestaltet werden, wie Schutzzweck der Norm und Eigenart der jeweiligen Akte es am sinnvollsten erscheinen lassen. Deshalb braucht z. B. ein in umfangreichen Akten mehrfach enthaltenes personenbezogenes Datum nicht an jeder einzelnen Stelle berichtigt zu werden; dies kann auch durch einen der Akte vorangestellten Vermerk geschehen.

In Absatz 2 Satz 1 Buchst. a bis c sind die Sperrungsfälle teilweise neu definiert: Während Buchst. a dem bisherigen Recht entspricht, kommt eine Sperrung nach Buchst. b angesichts der obligatorischen Löschungsverpflichtung nach Absatz 3 Satz 1 Buchst. a nur in den Fällen in Betracht, in denen der Betroffene ausdrücklich anstelle der Löschung die Sperrung verlangt (erklärter Wille); dies gilt nach Buchst. c in gleicher Weise, wenn die speichernde Stelle davon ausgehen muß, daß die Verwirklichung ihrer obligatorischen Löschungspflicht nach Absatz 3 dem Interesse des Betroffenen nicht entspricht, weil für ihn die Möglichkeit, noch auf die Daten zugreifen zu können, als vorrangig angesehen werden muß. Ein Anspruch des Betroffenen auf Sperrung besteht ferner, wenn die personenbezogenen Daten nur zu Zwecken der Datensicherung und der Datenschutzkontrolle gespeichert sind (Buchstabe d). Nach Absatz 1 Satz 2 sind die Gründe für die Sperrung nach Buchst. c aufzuzeichnen.

Absatz 2 Satz 3 gibt Hinweise für das Sperrungsverfahren bei automatisierter oder nicht-automatisierter Datenverarbeitung. Absatz 2 Satz 4 entspricht – abgesehen vom Fortfall der generellen Nutzungsberechtigung zu wissenschaftlichen Zwecken – dem bisherigen § 17 Absatz 2 Satz 3, 2. Halbsatz. Nutzung zu wissenschaftlichen Zwecken ist aber im Einzelfall bei überwiegendem Forschungsinteresse nach wie vor zulässig.

Nach Absatz 3 Satz 1 Buchst. a sind – wie bisher – personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig war. Mit der Einführung der obligatorischen Löschung nach Buchst. b wird die bisher in § 17 Absatz 3 enthaltene Regelung durch eine datenschutzfreundlichere Lösung ersetzt. Die bisherige Möglichkeit, anstelle der Sperrung nach § 17 Absatz 2 Satz 2 die Löschung nach Absatz 3 Satz 2, 2. Alternative zu verlangen, entfällt künftig, weil die Sperrung anstelle der Löschung nur noch unter den Voraussetzungen des neuen Absatzes 2 Satz 1, Buchst. b und c möglich ist.

Absatz 3 Satz 2 enthält eine Sonderregelung für Akten. Es wäre wenig sinnvoll, Akten fortwährend darauf durchsuchen zu müssen, ob in ihnen personenbezogene Daten enthalten sind, die nicht mehr benötigt werden und daher zu löschen sind. Zudem würde eine solche Löschung in vielen Fällen den Sachzusammenhang der Unterlagen zerstören. Deshalb soll bei Akten eine Löschung unter den Voraussetzungen des Absatzes 3 Satz 1 Buchst. b nur dann in Betracht kommen, wenn die gesamte Akte – vorbehaltlich archivrechtlicher Regelungen – nicht mehr zur Aufgabenerfüllung benötigt wird. Kommt eine Löschung noch nicht in Betracht, sind die personenbezogenen Daten auf Antrag des Betroffenen zu sperren (Teilsperrung).

Die obligatorische Verpflichtung der öffentlichen Stelle, nicht mehr zur Aufgabenerfüllung benötigte personenbezogene Daten in automatisierten Dateien, nicht-automatisierten Dateien oder Akten zu löschen, darf allerdings nicht das öffentliche Interesse an der Überlieferung historisch gewordener Vorgänge an die Nachwelt unmöglich machen. Absatz 4 eröffnet deshalb der speichernden Stelle die Möglichkeit, von einer Löschung nicht mehr benötigter personenbezogener Daten (Absatz 3 Satz 1, Buchst. b) in denjenigen Fällen abzusehen, in denen auf Grund von Rechtsvorschriften die Übernahme der gespeicherten Daten durch ein Archiv in Betracht kommt (Archivklausel).

Absatz 5 Satz 1 sieht eine Änderung und Erweiterung der bisher schon in § 17 Absatz 4 festgelegten Unterrichtungspflichten der speichernden Stelle vor. Diese Unterrichtungspflicht tritt künftig nicht nur in Fällen regelmäßiger Datenübermittlung ein, sondern auch bei den Einzelübermittlungen. Das informationelle Selbstbestimmungsrecht des Betroffenen ist nur dann in angemessenem Umfange gewahrt, wenn der Empfänger solcher Daten von den genannten erforderlich gewordenen Korrekturen Kenntnis erlangt und sich entsprechend verhalten kann.

Die Unterrichtung darf nach Satz 2 nur unterbleiben, wenn sie einen unverhältnismäßigen Verwaltungsaufwand erfordern würde und für den Betroffenen bei Unterlassung keine nachteiligen Folgen zu befürchten sind.

Die bisher in § 17 Abs. 5 vorgesehene Ermächtigung der Landesregierung zum Erlaß einer Verordnung über Löschungs- oder Sperrungsfristen soll aufgehoben werden. Solche Sperrungs- oder Löschungsfristen müßten die Aufbewahrungsdauer von Daten möglichst vieler Verwaltungsbereiche regeln; sachge-

recht können sie aber nur empirisch, bezogen auf das jeweilige Aufgabengebiet der Verwaltung oder sogar nur Teile davon festgelegt werden. Dies ist offenbar auch einer der Gründe, warum das Datenschutzgesetz selbst solche Löschungsfristen nicht vorgesehen hat.

Es soll daher künftig auf die der Landesregierung eingeräumte allgemeine Ermächtigung zur Festlegung solcher Sperrungs- und Löschungsfristen verzichtet werden. Erforderlichenfalls sind solche Ermächtigungen zum Erlaß entsprechender Rechtsverordnungen in den jeweiligen bereichsspezifischen Gesetzen vorzusehen.

Zu § 20 (Schadensersatz)

Schon bisher enthält das Datenschutzgesetz in § 4 Abs. 2 einen verschuldensunabhängigen Schadensersatzanspruch im Interesse eines möglichst umfassenden Schutzes des einzelnen im besonderen bei der automatisierten Datenverarbeitung. Für diese Regelung war die Erwägung maßgeblich, daß es dem einzelnen bei der Kompliziertheit der Technik und angesichts der Schwierigkeiten, die Vorgänge der Datenverarbeitung zu rekonstruieren, in der Regel nicht gelingen dürfte, den im Schadensersatzrecht erforderlichen Nachweis eines Verschuldens der datenverarbeitenden Stelle zu führen. Dabei hat sich der Gesetzgeber nicht für eine Umkehr der Beweislast, sondern für die Normierung eines Gefährdungshaftungstatbestandes entschieden. Diese Überlegungen erscheinen nach wie vor sachgerecht. Grundsätzlich tritt auch künftig die Haftung beim Einsatz von Datenverarbeitungsanlagen unabhängig von menschlichem Verschulden ein. Es besteht jedoch kein hinreichender Grund, diese Haftung auch für nicht automatisierte Dateien (Karteien), die ihrer Art nach eher den Akten vergleichbar sind, beizubehalten. Stattdessen soll bei schweren Fällen im Bereich der **automatisierten** Datenverarbeitung die Haftung der öffentlichen Stelle auch auf Schadensersatz für immaterielle Schäden erweitert werden. Darüber hinaus soll der Ersatzpflichtige dem Betroffenen für jedes schädigende Ereignis künftig bis zu einem Höchstbetrag von 500 000,– DM haften.

Für das Mitverschulden des Verletzten und für die Verjährung des Schadensersatzanspruchs sollen die §§ 254, 839 Abatz 3 und 852 des BGB Anwendung finden. Weitergehende verschuldensabhängige Schadensersatzansprüche bleiben – wie bisher – unberührt. Neben etwaigen vertraglichen Schadensersatzansprüchen kommen hier insbesondere die Ansprüche aus dem Gesichtspunkt der Staatshaftung gemäß Art. 34 GG, § 839 BGB bei hoheitlicher bzw. gemäß §§ 823, 31, 89 bzw. 831 BGB bei fiskalischer Tätigkeit in Betracht.

Zu § 21 (Berufung und Rechtsstellung)

Absatz 1 ist unverändert. Absatz 2 entspricht dem bisherigen § 24 Absatz 3.

In Absatz 3, der ansonsten dem bisherigen § 24 Absatz 2 entspricht, ist eine Ergänzung der Rechtsstellung des Landesbeauftragten vorgesehen: Der Landesbeauftragte ist auch oberste Dienstbehörde für die Entscheidung über die Vorlegung und Auslieferung von Akten seiner Behörde auf Grund von § 96 StPO; er trifft ferner die Entscheidungen nach den §§ 64 und 65 LBG (Aussagegenehmigung) für sich und seine Bediensteten in eigener Verantwortung

Absatz 4 entspricht dem bisherigen § 25 Absatz 1; Absatz 5 enthält eine Erweiterung des bisherigen § 25 Absatz 2. Der Absatz 6 entspricht dem bisherigen § 31 Absatz 3. Diese drei Absätze sind aus Gründen des Sachzusammenhangs künftig Bestandteil dieser Vorschrift.

Zu § 22 (Aufgaben)

Die Kontrolle der Einhaltung des Datenschutzes durch unabhängige Beauftragte für den Datenschutz stellt nach den Aussagen des Bundesverfassungsgerichts in seiner Entscheidung vom 15. Dezember 1983 eine wesentliche Voraussetzung dar, um das Recht des einzelnen auf informationelle Selbstbestimmung zu gewährleisten. In Nordrhein-Westfalen hat die Kontrollinstanz bereits seit 1978 Eingang in die Landesverfassung gefunden (vgl. Artikel 77a). Vor dem Hintergrund des Artikels 4 Absatz 2 der Landesverfassung, der den Schutz personenbezogener Daten unabhängig davon gewährleistet, auf welchen Datenträgern diese Daten gespeichert sind, sind Landesregierung und Landtag seit geraumer Zeit in der Absicht einig, die Rechte des Landesbeauftragten für den Datenschutz über die Dateien hinaus ausdrücklich auf die Kontrolle von Akten und sonstigen amtlichen Unterlagen zu erweitern.

Diesem Anliegen trägt der Entwurf auf Grund des durch § 2 Absatz 1 erweiterten gesetzlichen Anwendungsbereichs Rechnung, ohne daß es insoweit einer Änderung des Wortlautes des bisherigen § 26 Absatz 1 bedürfte. Künftig erstreckt sich die Kontrolle des Landesbeauftragten für den Datenschutz auf alle Formen der personenbezogenen Datenverarbeitung öffentlicher Stellen im Landesbereich. Die Kon-

trollbefugnis besteht auch nach wie vor für den Bereich der kommunalen Eigenbetriebe und sonstigen öffentlich-rechtlichen Unternehmen (vgl. zu § 2 Absatz 2); die materiellen Prüfungsmaßstäbe ergeben sich allerdings aus dem Bundesdatenschutzgesetz (dateimäßige Datenverarbeitung) sowie dem 3. Teil dieses Gesetzes.

Die Veränderungen in Absatz 1 sind bis auf die Einbeziehung des § 28 Absatz 4 redaktioneller Art; die bisher in § 26 Absatz 1 Satz 2 enthaltene Unterstützungsverpflichtung öffentlicher Stellen ist künftig im § 26 Absatz 1 Satz 1 enthalten.
Absatz 2 entspricht dem bisherigen § 26 Absatz 4.
Absatz 3 Satz 1 entspricht dem bisherigen § 26 Absatz 2.
Absatz 3 Satz 2 stellt sicher, daß die Belange des Datenschutzes schon bei der Planung des Landes zum Aufbau automatisierter personenbezogener Informationssysteme berücksichtigt werden. Dies erfordert eine rechtzeitige Einflußnahme des Landesbeauftragten auf die datenschutzgerechte Ausgestaltung solcher Systeme.
Absatz 4 entspricht dem bisherigen § 31 Absatz 2.
Absatz 5 entspricht dem bisherigen § 28; nur redaktionelle Anpassung.
Absatz 6 entspricht dem bisherigen § 26 Absatz 5. Die bisher in § 26 Absatz 6 enthaltene Amtshilfeverpflichtung entfällt im Hinblick auf die Fassung des § 26 Absatz 1 Satz 1.

Zu § 23 (Dateienregister)

Die Vorschrift ist weitgehend völlig neu konzipiert. Die bisherigen Absätze 1 bis 5 des § 27 werden durch die Regelungen in den neuen Absätzen 1 und 2 ersetzt.

Abweichend von § 27 Absatz 1 Satz 1, der bisher eine Registerführung des Landesbeauftragten für **alle** Dateien (automatisiert und nicht-automatisiert) vorsah, beschränkt sich die Meldepflicht der speichernden Stelle und die Registerführung nach Absatz 1 Sätzen 1 und 2 künftig auf die **automatisiert geführten Dateien.** Diese Beschränkung der Registerpflicht öffentlicher Stellen wird durch die in § 8 (Dateibeschreibung) getroffene Regelung möglich: Danach haben alle datenverarbeitenden öffentlichen Stellen unabhängig von ihrer Pflicht zur Registermeldung die bei ihnen verwalteten Dateien – ob in automatisierter oder konventioneller Form – zu Zwecken der Selbstkontrolle in der Dateibeschreibung zu erfassen. Ausnahmen gelten nur für die interne Datei sowie Hilfs- und Zwischendateien. Diese verstärkte Selbstkontrolle der Verwaltung läßt daher für nicht-automatisierte Dateien einen Verzicht auf die Pflicht zur Registeranmeldung zu.

Dieses primär zur Selbstkontrolle der datenverarbeitenden Stelle bestimmte Organisationsinstrument bildet gleichzeitig die Grundlage für das Dateienregister und erlaubt darüber hinaus eine umfassende externe Kontrolle des Landesbeauftragten. Die speichernden Stellen (einschließlich der sog. Wettbewerbsunternehmen) sind verpflichtet, für alle automatisiert geführten Dateien entsprechende Angaben nach der Dateibeschreibung vorzulegen. Ausnahmen (ganz oder teilweise) von der Meldepflicht für bestimmte Behörden gibt es in Zukunft nicht mehr (vgl. bisher § 27 Absatz 2 Satz 2 und Absatz 4 Satz 1). Das Dateienregister muß für automatisierte Verfahren lückenlos sein. Die Kenntnis der **automatisiert vorgehaltenen** Dateien ist eine wesentliche Voraussetzung für die Ausübung der Kontrolltätigkeit des Landesbeauftragten, zumal deren Anzahl infolge der sich abzeichnenden technischen Entwicklung immer mehr zunehmen wird. Einschränkungen sind für bestimmte Dateien nur beim Auskunfts- bzw. Einsichtsrecht vertretbar.

Nach Absatz 2 Satz 1 wird das bisherige Registereinsichtsrecht durch jedermann (§ 27 Absatz 1 Satz 2) in Zukunft in erster Linie durch das generelle Recht auf schriftliche Auskunft aus dem Register des Landesbeauftragten für den Datenschutz abgelöst. Das bisherige Einsichtsrecht ist unter den in Nordrhein-Westfalen gegebenen Verhältnissen teilweise anachronistisch. Voraussetzung für den Anspruch auf schriftliche Auskunft ist, daß der Antragsteller ein berechtigtes Interesse an der Kenntnis der automatisierten Dateien darlegt; die Auskunft erfolgt unentgeltlich.

Daneben bleibt die Möglichkeit einer persönlichen Einsichtnahme des Registers durch den Betroffenen erhalten (Satz 2). Nach Satz 3 gibt es aber weder Auskunfts- noch Einsichtsrechte bezüglich der automatisierten **Dateien** der Sicherheitsbehörden sowie der öffentlich-rechtlichen Wettbewerbsunternehmen (bisher § 27 Absatz 4 Satz 3 und Absatz 5 Satz 2).

Absatz 3 sieht – wie bisher – eine Rechtsverordnungsermächtigung für die Landesregierung vor.

Zu § 24 (Beanstandungen durch den Landesbeauftragten)

Die Regelung entspricht bis auf die Änderung in Absatz 1 Satz 1 Ziffer 3 und bis auf redaktionelle Verbesserungen dem bisherigen § 30.

Die materielle Änderung ist eine Folge der Änderung von § 2 Absatz 2 Satz 2.

Die Erweiterung in Absatz 2, 2. Halbsatz räumt dem Landesbeauftragten die Möglichkeit ein, das Recht auf Beanstandung und das Verfahren noch flexibler zu handhaben. Zugleich erhalten die Behörden einen Anreiz, festgestellte Mängel unverzüglich zu beseitigen, weil sie auf dieser Weise einer förmlichen Maßnahme des Landesbeauftragten für den Datenschutz begegnen können.

Zu § 25 (Anrufungsrecht des Betroffenen)

Die redaktionell neugestaltete Vorschrift entspricht inhaltlich im wesentlichen dem bisherigen § 29. Absatz 1 Satz 1, 2. Halbsatz enthält eine Klarstellung für den öffentlichen Dienst. Der neue Absatz 2 enthält ein allgemeines Benachteiligungsverbot.

Zu § 26 (Durchführung der Kontrolle)

Absatz 1 faßt die bisher in § 26 Absatz 1 Satz 2, Absatz 3 und Absatz 6 enthaltenen Regelungen zusammen. Danach sind alle öffentlichen Stellen verpflichet, den Landesbeauftragten für den Datenschutz bei seiner Kontrolltätigkeit zu unterstützen. Diese Unterstützungspflicht gilt nicht nur in den Fällen, in denen der Landesbeauftragte bei der betreffenden öffentlichen Stelle selbst seine Kontrolltätigkeit ausübt, sondern auch, wenn sie der Amtshilfe zuzurechnen ist. Beispielhaft sind besonders wichtige Einzelpflichten aufgeführt.

Der Absatz 2 läßt eine Beschränkung der Informations- und Kontrollrechte des Landesbeauftragten für den Datenschutz nur unter ganz besonderen Voraussetzungen im Einzelfall zu.

Zu § 27 (Tätigkeitsberichte)

Die neue Regelung knüpft an den bisherigen § 31 Absatz 1 an. Nachdem die Einführungs- und Konsolidierungsphase des am 1. Januar 1979 in Kraft getretenen Datenschutzgesetzes NRW nach über sieben Jahren abgeschlossen ist, besteht Anlaß, die Berichterstattung des Landesbeauftragten und die Stellungnahme der Landesregierung neu zu regeln und flexibler zu gestalten. Dieses Ziel soll durch eine Verlängerung des Berichtszeitraums verwirklicht werden, damit soll gleichzeitig eine Berichtspflicht der Landesregierung über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden verbunden werden. Als Berichtszeitraum sollte das Kalenderjahr angestrebt werden; deshalb ist auf das bisherige Vorlagedatum für den Tätigkeitsbericht des Landesbeauftragten für den Datenschutz verzichtet worden.

Zu § 28 (Datenverarbeitung für wissenschaftliche Zwecke)

Die Verarbeitung personenbezogener Daten zu Zwecken wissenschaftlicher Forschung durch öffentliche Stellen einschließlich der Datenübermittlungen an private Forschungsstellen bedarf der gesetzlichen Regelung. Die Erarbeitung einer solchen Regelung im Rahmen einer allgemeinen Forschungsklausel muß die sich prinzipiell gegenüberstehenden Interessen in Einklang bringen: Den sachgerechten Ausgleich zwischen den Erfordernissen der Forschung im Interesse der Allgemeinheit und dem unerläßlichen Schutz des einzelnen bezüglich seiner zum Teil äußerst sensitiven personenbezogenen Daten. Die unter dem Begriff wissenschaftliche Forschung zusammengefaßten Sachverhalte sind jedoch unterschiedlich, insbesondere auch hinsichtlich der jeweils in Betracht kommenden Eingriffstiefe. Die neue Vorschrift will daher nur die allgemeinen Grundprinzipien aufzeigen, nach denen das Spannungsverhältnis zwischen Forschung und informationellem Selbstbestimmungsrecht des einzelnen gelöst werden kann; ergänzende oder modifizierende bereichsspezifische Datenschutzregelungen werden dadurch nicht ohne weiteres verzichtbar.

Personenbezogene Daten sind häufig von wesentlicher, manchmal sogar von ausschlaggebender Bedeutung bei der Forschung. Soziologische Untersuchungen mit ihren Fragebogen und Interviews stellen ein besonders deutliches Beispiel für das Interesse an personenbezogenen Informationen dar. Aber auch die Erforschung bestimmter epidemiologischer Krankheiten und der Wirksamkeit bestimmter Behandlungen zeigen klar, bis zu welchem Grad die Forschung auf den Zugang zu Informationen über das individuelle Verhalten einer Person angewiesen ist. Für den Bereich der Psychologie und der Erziehungswissenschaften lassen sich vergleichbare Feststellungen treffen. Umfangreiche Sektoren der Forschung hängen deshalb, auch wenn die Disziplinen andere sind, von Informationselementen über identifizierbare Personen ab.

Bis vor etwa 10 Jahren wurde eine besondere Rechtfertigung zur Verwendung solcher personenbezogener Daten im Rahmen von Forschungsvorhaben nicht verlangt. Die einfache Tatsache, daß Daten für die

Forschung notwendig waren, reichte aus und im Hinblick auf gelegentlich geäußerte Kritik wurde insbesondere im medizinischen Bereich auf die berufsethischen Vorschriften mit ihrer langen Tradition verwiesen. Zwar wurde die Notwendigkeit von Kontrollmechanismen mehr oder weniger von den Forschern anerkannt, gleichzeitig aber als ein rein internes Problem angesehen, das im Wege der Selbstregelung gelöst werden sollte. Diese Selbstregelungen erwiesen sich jedoch nicht als geeigneter Weg, die erhebliche Rechtsunsicherheit auszuräumen. Es blieb daher notwendig, gesetzgeberische Schritte zu unternehmen, die durch Selbstregelung vervollständigt aber nicht ersetzt werden können. Solche gesetzgeberischen Schritte wurden bereits mit früheren Vorschlägen zur Novellierung der allgemeinen Datenschutzgesetze eingeleitet; sie haben sich in Nordrhein-Westfalen bereits mit dem sog. Krebsregistergesetz konkretisiert und finden für den medizinischen Bereich zunehmend auch ihren Niederschlag in Krankenhausgesetzen. Dabei werden den Forschungsinteressen keine prinzipiellen Vorrechte vor dem Datenschutz zugestanden: Die Forschung wird an dieselben Grundregeln gefunden, welche die Verwendung personenbezogener Daten auch durch andere Stellen mit sich bringt.

Das Datenschutzgesetz Nordrhein-Westfalen enthält im Gegensatz zum Bundesdatenschutzgesetz schon bisher in § 12 eine Regelung über die Zulässigkeitsvoraussetzungen wissenschaftlicher Datenverarbeitung. Es läßt für Hochschulen und vergleichbare öffentliche Einrichtungen Speicherung und Veränderung personenbezogener Daten im Rahmen ihrer Aufgaben für bestimmte Forschungsvorhaben zu und legitimiert auch die dazu im Einzelfall erforderlichen Datenübermittlungen durch andere öffentliche Stellen. Entscheidende Zulässigkeitsvoraussetzung dieser Datenverarbeitung ist schon heute, daß die Einwilligung des Betroffenen vorliegt oder jedenfalls feststeht, daß seine schutzwürdigen Belange nicht beeinträchtigt werden. Diese Regelung wird durch eine spezielle Anzeigepflicht der übermittelnden Stelle ergänzt und durch das Verbot der Weiterübermittlung solcher Daten ohne Einwilligung des Betroffenen.

Auf europäischer Ebene läßt auch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten eine Verarbeitung bestimmter sensitiver Daten (z. B. politische und religiöse Überzeugung, Gesundheitsdaten) nur zu, wenn das innerstaatliche Recht einen geeigneten Schutz gewährleistet (Artikel 6; Gesetz zu dem Übereinkommen vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 13. März 1985 – BGBl. II S. 538 ff.). Von Bedeutung ist in diesem Zusammenhang auch die Empfehlung des Europarates zum Schutze personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik, die in der 362. Sitzung der Ministerbeauftragten vom 14. bis 23. September 1983 einstimmig angenommen worden ist. Daß diese Bestrebungen durch die Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 auch innerstaatlich zusätzliche Bedeutung gewonnen haben, bedarf keines weiteren Nachweises. Unbestritten ist danach, daß sich die Forschung denselben Grundregelungen zu unterwerfen hat wie andere Bereiche auch, die personenbezogene Daten im Rahmen ihrer Aufgabenerfüllung verarbeiten. Gleichwohl sind bei der Abwägung der Forschungsinteressen mit dem unerläßlichen Schutz der Privatsphäre des einzelnen die mit der Datenverarbeitung verfolgten Ziele und die Struktur der Informationsprozesse zu berücksichtigen. Dies führt – jedenfalls im Rahmen einer allgemeinen Forschungsklausel – zu einer gestuften Regelung. Die neue Vorschrift will deshalb die bisherigen Zulässigkeitskriterien keineswegs aufgeben, orientiert sich aber noch stärker am informationellen Selbstbestimmungsrecht und unternimmt es dabei, die einzelnen Sachverhalte stärker zu differenzieren und zu präzisieren, als das im bisherigen § 12 der Fall ist. Dabei wird unterschieden zwischen der eigenen Datenverarbeitung öffentlicher Stellen zu Zwecken wissenschaftlicher Forschung und der Übermittlung personenbezogener Daten an andere öffentliche oder auch nicht-öffentliche Forschungsstellen. Im einzelnen gilt folgendes:

Entsprechend dem informationellen Selbstbestimmungsrecht dürfen nach Absatz 1 Satz 1 personenbezogene Daten von öffentlichen Stellen zur Durchführung eines bestimmten Forschungsvorhabens grundsätzlich nur verarbeitet werden, wenn der Betroffene hierzu sein Einverständnis erklärt hat. Zu einem Konflikt zwischen dem Persönlichkeitsrecht des einzelnen und den Interessen der Forschung kommt es in diesem Falle nicht, weil der Berechtigte seine eigenen Daten der wissenschaftlichen Forschung zur Verfügung stellt. Für die Einholung der Einwilligung des Betroffenen sind dabei die in § 4 neugefaßten und erweiterten Aufklärungs- und Belehrungspflichten zu beachten. Für die Übermittlungsphase gilt dabei die Sonderregelung in Absatz 2. Der Entwurf geht damit konzeptionell von der Vorstellung aus, daß der Einwilligungslösung (sog. aufgeklärte Einwilligung) in Zukunft Priorität zukommt. Ein ganz erheblicher Teil aller Fälle läßt sich über die Einwilligung lösen; bekanntlich machen davon bereits verschiedene Einrichtungen im medizinischen Bereich Gebrauch, ohne daß es deshalb zu einer ernsthaften Behinderung der Forschung gekommen wäre. Allerdings setzt dies einen gewissen Umdenkungsprozeß der Beteiligten voraus, der dem informationellen Selbstbestimmunsrecht ein größeres Gewicht beimißt.

Gleichwohl ist es nicht in allen Fällen möglich und auch nicht notwendig, die Einwilligung des Betroffenen einzuholen. Mit der Einholung der Einwilligung können subjektive Auswirkungen verbunden sein, die dem Betroffenen die Erteilung der Einwilligung nicht zumutbar erscheinen lassen. Aber auch objektive Schwierigkeiten können der Einholung der Einwilligung entgegenstehen oder diese in unverhältnismäßiger Weise erschweren. Solche Konflikte zwischen Belangen der Forschung und dem Recht auf informationelle Selbstbestimmung versucht zunächst Absatz 1 Satz 2 in der Weise zu lösen, daß die Verarbeitung personenbezogener Daten für die Forschung durch bestimmte Personen innerhalb öffentlich-rechtlicher Organisationseinheiten besonders geregelt wird (sog. interne Forschung). Die Regelung ermöglicht den Ressorts und den Verwaltungen, aber auch sonstigen öffentlichen Stellen, interne Quellen zu Forschungszwecken zu nutzen. Die potentielle Gefährdung des Betroffenen erscheint hier gering, weil die datenverarbeitenden Stellen und damit die Forscher bereits im Rahmen ihrer Zuständigkeiten rechtmäßigen Zugriff auf den jeweiligen Datenbestand haben. Unter dieser Voraussetzung wird es für vertretbar gehalten, die mit der Verwendung der Daten zu Forschungszwecken verbundene Zweckänderung auch ohne Einwilligung des Betroffenen zuzulassen. Weitere Voraussetzung ist dabei, daß die Zweckänderung im öffentlichen Interesse liegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann, d.h. das Forschungsvorhaben mit Hilfe anonymisierter Daten nicht realisierbar ist. Dann dürfen Daten in personenbezogener Form auch ohne Einwilligung des Betroffenen verarbeitet werden. Allerdings ist ferner darauf hinzuweisen, daß der Begriff „öffentliche Stelle" nur spezifische und genau umrissene Organisationseinheiten erfaßt und nicht etwa die Gesamtheit aller öffentlichen Stellen eines Aufgabenträgers. Mit einer solchen „in house research"-Regelung kann vor allem im medizinischen Bereich ein erheblicher Teil der Forschungstätigkeit erfaßt werden (beispielsweise in den Universitätskliniken).

Nach Absatz 1 Satz 3 bedarf es außerhalb der internen Forschung keiner Einwilligung der Betroffenen, wenn dem informationellen Selbstbestimmungsrecht besondere, überragende Gemeinschaftsinteressen gegenüberstehen: Das öffentliche Interesse an der Durchführung des Forschungsvorhabens muß das Geheimhaltungsinteresse des Betroffenen überwiegen.

In einem solchen Fall sind jedoch besondere Kontrollmechanismen notwendig, um die – anstelle der Einwilligung – erforderliche Güterabwägung zu gewährleisten. Nach Absatz 1 Satz 4 soll deshalb die Verarbeitung personenbezogener Daten durch Behörden und Einrichtungen des Landes eine Unterrichtungspflicht an die zuständigen obersten Landesbehörden oder eine von dieser bestimmten Stelle auslösen. Um jede Gefahr eines Mißbrauchs soweit wie möglich auszuschließen, sollen die übrigen öffentlichen Stellen in den Fällen wissenschaftlicher Datenverarbeitung ohne Einwilligung des Betroffenen nach Satz 3 den Landesbeauftragten für den Datenschutz unterrichten, damit dieser von den ihm zustehenden Kontrollmöglichkeiten ggfs. unverzüglich Gebrauch machen kann.

Absatz 2 enthält entsprechende Regelungen für die Übermittlung. Zunächst sind Datenübermittlungen zu Forschungszwecken analog der Regelung in Abatz 1 Satz 1 mit Einwilligung des Betroffenen immer zulässig, wobei an die Einwilligung ebenfalls die Anforderungen des § 4 anzulegen sind. Ohne Einwilligung des Betroffenen sind Datenübermittlungen (im Sinne des § 3 Absatz 2 Satz 2 Nr. 4 i.V.m. § 3 Absatz 3) nur dann zulässig, wenn die Voraussetzungen des Absatzes 1 Satz 3 vorliegen, d.h. überragende Gemeinschaftsinteressen den Vorrang vor dem informationellen Selbstbestimmungsrecht verdienen. Für Stellen des Landes gilt darüber hinaus, daß Datenübermittlungen in den letztgenannten Fällen die Unterrichtungspflicht entsprechend § 1 Satz 4 auslösen; in den übrigen Fällen gilt die besondere Informationsverpflichtung zugunsten des Landesbeauftragten auch hier. Nach Absatz 2 Satz 2 gilt hier ein strenges Zweckbindungsgebot: Eine anderweitige Verwendung der übermittelten Daten ist unzulässig, es sei denn mit ausdrücklicher Einwilligung des Betroffenen. Absatz 3 sieht darüber hinaus eine möglichst frühzeitige Anonymisierung der verwendeten personenbezogenen Daten vor. Zum frühestmöglichen Zeitpunkt soll der Bezug der Daten zu bestimmten natürlichen Personen aufgelöst und damit der Schutz des Betroffenen verstärkt werden. Diese Regelung entbindet allerdings nicht von der grundsätzlichen Pflicht zu prüfen, ob das Forschungsvorhaben nicht überhaupt ohne Bezug auf eine bestimmte natürliche Person durchgeführt werden kann (vgl. Absatz 1 Satz 2).

Als Mittel der Deanonymisierung dienen die gesonderte Speicherung der Zusatzmerkmale nach Satz 2 und ihre spätere Löschung, sobald der Forschungszweck dies gestattet. Absatz 4 trägt dem Umstand Rechnung, daß sich die Gesetzgebungskompetenz des Landes nicht direkt auf private Stellen erstreckt. An Privatpersonen oder andere nicht-öffentliche Stellen dürfen personenbezogene Daten zu Forschungszwecken nur unter zusätzlichen Bedingungen übermittelt werden. Diese Stellen müssen sich verpflichten, die personenbezogenen Daten nur zu den bei der Übermittlung vorliegenden Forschungszwekken zu nutzen und die personenbezogenen Daten sobald wie möglich zu anonymisieren. Gleichzeitig müssen sie sich im Landesbereich mit der Kontrolle durch den Landesbeauftragten für den Datenschutz einverstanden erklären. Bei Datenübermittlungen für Forschungsvorhaben außerhalb des Geltungsbereichs dieses Gesetzes ist generell die zuständige Datenschutzkontrollbehörde zu unterrichten.

Absatz 5 trifft eine neue Regelung über die Befugnisse zur Veröffentlichung personenbezogener Daten im Rahmen wissenschaftlicher Forschung. Sie wird an enge Zulässigkeitsvoraussetzungen gebunden: Prinzipiell ist die Einwilligung des Betroffenen erforderlich; nur in den Fällen, in denen die Veröffentlichung personenbezogener Daten für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerläßlich ist, soll das informationelle Selbstbestimmungsrecht gegenüber dem zeitgeschichtlichen Interesse zurücktreten. Damit ergeben sich Berührungspunkte zu möglichen Archivregelungen.

Zu § 29 (Datenverarbeitung bei Dienst- und Arbeitsverhältnissen)

Die neue Vorschrift regelt die Besonderheiten der Datenverarbeitung bei dienst- oder arbeitsrechtlichen Beschäftigungsverhältnissen im Bereich der öffentlichen Verwaltung. Für das Verhältnis dieser Bestimmung (und der übrigen Sonderbestimmungen des Dritten Teils) zu den übrigen Vorschriften des Gesetzes gilt: Neben § 29 sind auch die übrigen Vorschriften ohne Ausnahme anzuwenden, soweit diese Bestimmung nicht bei gleichem Sachverhalt eine abweichende Regelung (z. B. für die Löschung) trifft, wodurch die allgemeine Vorschrift verdrängt wird. § 29 seinerseits findet insoweit gemäß § 2 Absatz 3 keine Anwendung, als bereichsspezifische Normen (z. B. § 102 LBG, Personalakteneinsichtsrecht des Beamten) mit entsprechendem Regelungsgehalt den Vorschriften des Datenschutzgesetzes vorgehen. Voraussetzung ist dafür allerdings, daß die bereichsspezifischen Normen – jedenfalls in Zukunft – verfassungsrechtlichen Erfordernissen genügen.

Verarbeitung personenbezogener Daten der Bediensteten durch den Dienstherrn bei der Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses stellt einen Eingriff in das informationelle Selbstbestimmungsrecht dar: Ein solcher Umgang mit personenbezogenen Daten bedarf deshalb der gesetzlichen Ermächtigung (Absatz 1 Satz 1). Dies gilt auch für die Durchführung bestimmter dienstbezogener Maßnahmen, sowie insbesondere auch für Personalplanung und -einsatz. Insbesondere die in den letzten Jahren zu beobachtende Zunahme der Anzahl von automatisch geführten Dateien mit Arbeitnehmerdaten (sog. Personalinformationssysteme), die eine Nutzung zu den verschiedensten Zwecken (multifunktionale Nutzung) ermöglichen, erfordert eine solche prinzipielle Grundentscheidung des Gesetzgebers. Für alle Fälle ist deshalb zwingende Voraussetzung, daß die Datenverarbeitung entweder dem strengen Grundsatz der Erforderlichkeit entspricht oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung diese vorsehen. Nur unter diesen Voraussetzungen dürfen Angaben über berufliche und fachliche Qualifikationen (Einstellungsvoraussetzungen, Erfahrungen und Fähigkeiten, Beurteilungen) verarbeitet werden; dies gilt auch für Angaben über persönliche und wirtschaftliche Verhältnisse des Beschäftigten, soweit daran im Hinblick auf die zu leistende Tätigkeit ein berechtigtes Interesse des Dienstherrn besteht.

Eine Übermittlung personenbezogener Daten an einen künftigen Dienstherrn oder Arbeitgeber soll in Zukunft nur noch mit Einwilligung des Betroffenen zulässig sein (Absatz 1 Satz 2). Eine Übermittlung solcher Daten nach § 16 Absatz 1 Buchstabe c bleibt unter den dort genannten besonderen Voraussetzungen zulässig; hier handelt es sich nicht um dienstbezogene Übermittlungen, sondern um Auskunftsersuchen privater Dritter, die ein rechtliches Interesse geltend machen. Auch die Weiterverarbeitung personenbezogener Daten aus ärztlichen oder psychologischen Untersuchungen und Tests zum Zwecke des Abschlusses eines Dienst- oder Arbeitsverhältnisses sind nach Absatz 2 Satz 1 ausdrücklich an die Einwilligung des Bewerbers gebunden. Selbstverständlich gilt dies auch für die Untersuchung selbst. Dabei richten sich die Voraussetzungen ärztlicher oder psychologischer Untersuchungen nach den jeweils bestehenden materiell-rechtlichen Vorschriften. Die öffentliche Stelle darf vom untersuchenden Dritten nach Absatz 2 Satz 2 in der Regel nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und festgestellter Risikofaktoren verlangen, soweit nicht besondere Gründe eine Mitteilung über das gesamte Untersuchungsergebnis notwendig machen. Dies wird z. B. bei der Einstellung in den Polizeivollzugsdienst erforderlich sein. Insgesamt wird dadurch ein stärkerer Schutz der Gesundheitsdaten erreicht.

Dem verstärkten Schutz des Bewerbers dient auch die in Absatz 3 Satz 1 vorgesehene besondere Verpflichtung der öffentlichen Stelle, erhobene Daten unverzüglich zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, es sei denn, daß der Betroffene in die weitere Speicherung ausdrücklich eingewilligt hat. Soweit bundesrechtliche Vorschriften (z. B. Röntgenverordnung) eine Aufbewahrung bestimmter Daten vorschreiben, bleiben diese unberührt. Nach Beendigung eines Dienst- oder Arbeitsverhältnisses besteht eine obligatorische Verpflichtung nach Absatz 3 Satz 2, personenbezogene Daten zu löschen, wenn diese Daten nicht mehr benötigt werden und es sei denn, daß keine Rechtsvorschriften der Löschung entgegenstehen. Eine weitere Einschränkung der Löschungspflicht kann sich aber auch in diesen Fällen aus § 19 Absatz 3 Satz 2 und Absatz 4 ergeben.

In Absatz 4 Satz 1 wird die automatisierte Verarbeitung personenbezogener Daten aus medizinischen oder psychologischen Untersuchungen oder Tests des Beschäftigten beschränkt. Eine solche technische Verarbeitung der erhobenen Daten soll nur zulässig sein, wenn sie – zumindest auch – dem Schutz des Beschäftigten dient. Von ähnlichen Überlegungen geht die weitere Regelung in Absatz 4 Satz 2 aus, wonach dienstliche Beurteilungen nicht allein auf unmittelbare Computerinformationen gestützt werden dürfen. Dadurch soll verhindert werden, daß der Betroffene zum Objekt des Computers entwürdigt wird. Ihr Vorbild findet diese Vorschrift in Artikel 2 des französischen Datenschutzgesetzes.

Absatz 5 stellt schließlich sicher, daß die gespeicherten Daten von Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Sicherungsmaßnahmen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden. Ansonsten träte auch eine Ungleichbehandlung gegenüber den Beschäftigten ein, die nicht an Datenverarbeitungsgeräten tätig sind.

Zu § 30 (Fernmessen und Fernwirken)

Die neue Vorschrift trifft erstmals generelle Bestimmungen über die Zulässigkeit der Einrichtung von Fernmeß- und Fernwirkdiensten durch öffentliche Stellen oder öffentliche Wettbewerbsunternehmen in Wohnungen oder Geschäftsräumen Privater. Dieser erhebliche Eingriff in das informationelle Selbstbestimmungsrecht ist nach Absatz 1 Sätze 1 und 2 nur zulässig, wenn der Betroffene nach einer im einzelnen vorgeschriebenen Unterrichtung durch die einrichtende Stelle seine Einwilligung schriftlich erklärt hat. Der Betroffene muß ferner erkennen können, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist (Satz 3). Dies gilt nicht für Einrichtungen von Versorgungsunternehmen. Der Betroffene kann darüber hinaus die Einwilligung jederzeit widerrufen; dies muß allerdings mit der Zweckbestimmung des Dienstes vereinbar sein. Im Zweifel gilt das Abschalten des Dienstes als Widerruf (Absatz 1 Sätze 4 und 5).

Nach Absatz 2 Satz 1 besteht ein Junktimverbot, die vertragliche Leistung, den Abschluß oder die Abwicklung des Vertragsverhältnisses von der Einwilligung des Betroffenen zur Einrichtung der Dienste abhängig zu machen. Damit soll die Entscheidungsfreiheit des Betroffenen soweit wie möglich gewahrt bleiben. Ihn dürfen nur die unmittelbaren Kosten der Verweigerung oder des Widerrufs treffen (Nachteilsverbot – Satz 2).

Nach Absatz 3 Sätzen 1 und 2 gilt strenge Zweckbindung bei der Verarbeitung personenbezogener Daten und ein obligatorisches Löschungsgebot.

Zu § 31 (Nutzung von Verwaltungsdaten für die Erstellung von Statistiken)

Die neue Vorschrift stellt eine besondere Datenschutzregelung dar, der aber genereller Charakter zukommt; sie will den öffentlichen Stellen die Verwendung und Nutzung der bei diesen bereits angefallenen personenbezogenen Daten für Zwecke der Statistik (Aggregierung) ermöglichen. Im Rahmen der Aufgabenerfüllung fallen in vielen Bereichen der Verwaltung personenbezogene Daten an, deren statistische Auswertung in der Regel mit einer Zweckänderung der ursprünglich für bestimmte Aufgaben erhobene Daten verbunden ist. Auf solche Auswertungen kann die Verwaltung, etwa zur Erstellung von Geschäftsstatistiken, nicht verzichten. Das ursprünglich personenbezogene Datenmaterial wird als „statistische Masse" zur Aggregierung (Zusammenfassung) gleichartig zuzuordnender statistischer Mengen genutzt. Die Bedeutung einer solchen Nutzung personenbezogener Daten ist erheblich: Solche Statistiken dienen nicht nur der Beobachtung der Entwicklung des Geschäftsanfalls als solcher (Geschäftsstatistiken), sondern vielfach auch inhaltlichen Analysen über die sachliche Entwicklung des betreffenden Rechtsprechungs- oder Verwaltungsbereichs. Insbesondere im kommunalen Bereich kommt diesen Statistiken Bedeutung zu, weil sie dazu dienen können, Aufschlüsse über die wirtschaftliche und soziale Entwicklung sowie über die kulturellen und ökologischen Erfordernisse zu geben. Die damit zwangsläufig verbundene Beeinträchtigung des informationellen Selbstbestimmungsrechts ist als verhältnismäßig gering einzustufen. Satzt 1 legitimiert daher die Auswertung und Nutzung derartiger personenbezogener Daten ausschließlich für Zwecke der Erstellung von Statistiken, aus denen – jedenfalls ohne Zusatzwissen – ein Personenbezug nicht mehr hergestellt werden kann.

Ergänzt werden die dadurch geschaffenen Informationsmöglichkeiten für die Kommunen durch die Nutzung von Einzelangaben aus der amtlichen Statistik (vgl. Zu § 32) und die – schon von Kommunen genutzte – Möglichkeit, statistische Daten im Rahmen einer Befragung mit Einwilligung der Bürger zu erhalten.

Satz 2 legt einschränkend fest, daß die Veröffentlichung solcher Statistiken keine Angaben enthalten darf, die eine Identifizierung natürlicher Personen (Deanonymisierung) ermöglicht.

Zu § 32 (Nutzung von Einzelangaben aus der amtlichen Statistik durch Gemeinden und Gemeindeverbände)

Auf dem Hintergrund der Aussagen des Bundesverfassungsgerichts im sog. Volkszählungsurteil vom 15. 12. 1983 – BVerfGE Bd. 65, S. 1 ff. (61 f., 66/69) bestimmt § 14 Abs. 1 des Volkszählungsgesetzes 1987, daß Einzelangaben aus der Volkszählung den für die Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbände für ihren Zuständigkeitsbereich (nur) übermittelt werden dürfen

- für ausschließlich statistische Aufgaben
- ohne Hilfsmerkmale (d. h. Vor- und Familiennamen, Straße und Hausnummer, Name der Arbeits- oder Ausbildungsstätte – vgl. § 8 VZG –)
- auf Datenträgern, die für die maschinelle Weiterverarbeitung bestimmt sind,
- höchstens auf der Grundlage von Blockseiten

und wenn durch Landesgesetz eine Trennung der zur Durchführung statistischer Aufgaben zuständigen Stelle von anderen kommunalen Verwaltungsstellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist.

Die letztgenannten, dem Landesgesetzgeber zugewiesenen Voraussetzungen sollen durch die neue Vorschrift geschaffen werden. Sie ist so gefaßt, daß sie über das Volkszählungsgesetz 1987 hinaus in zukünftigen Fällen, in denen durch den Gesetzgeber eine Weiterleitung von formal anonymisierten Datensätzen an Gemeinden und Gemeindeverbände zugelassen wird, in gleicher Weise das Statistikgeheimnis sichert. In Anlehnung an § 14 Abs. 1 Volkszählungsgesetz 1987 ist daher in Absatz 1 festgelegt, daß Einzelangaben (Datensätze) weitergegeben werden können, wenn dies auf Grund gesetzlicher Ermächtigung zulässig ist und auf Datenträgern geschieht, die zur maschinellen Weiterverarbeitung bestimmt sind.

Absatz 2 legt die Voraussetzungen der vom Bundesverfassungsgericht geforderten „Abschottung" und „informationellen Gewaltenteilung" fest: Die Datenträger dürfen nur unmittelbar der für die Durchführung statistischer Aufgaben zuständigen Stelle der Gemeinde oder des Gemeindeverbands übermittelt werden und nur dann, wenn diese

- organisatorisch und räumlich von den übrigen Verwaltungsstellen der Körperschaft getrennt ist,
- gegen den Zutritt unbefugter Personen hinreichend geschützt ist,
- und mit eigenem Personal ausgestattet ist, das die Gewähr für Zuverlässigkeit und Verschwiegenheit bietet, schriftlich auf das Statistikgeheimnis verpflichtet und während der Tätigkeit in der Statistikdienststelle nicht mit anderen Aufgaben des Verwaltungsvollzugs betraut ist.

Diese Regelungen zur organisatorischen, räumlichen und personellen Abschottung werden in Absatz 3 ergänzt durch ein personenbezogenes Zweckentfremdungsverbot.

Für die Nutzung der nach Absatz 1 übermittelten Datensätze aus der amtlichen Statistik trägt Absatz 4 der Tatsache Rechnung, daß nach Auffassung des Bundesverfassungsgerichts im kommunalen Bereich die Grenzen statistischer Nutzung fließend sind, daß aber gleichwohl eine Zweckbindung an die Durchführung statistischer Aufgaben sicherzustellen ist. Im Hinblick auf die vom Bundesverfassungsgericht betonte Gefährdung des Rechts auf informationelle Selbstbestimmung bei kleinräumiger Aufbereitung und dem bei den Gemeinden und Gemeindeverbänden vorhandenen besonders großen Zusatzwissen wird als „statistische Nutzung" die Aggregierung der Einzelangaben zu gleichartigen objektiven mengenmäßigen Gesamtheiten verstanden, aus denen ein Personenbezug nicht wiederhergestellt werden kann.

Absatz 4 Satz 2 stellt insbesondere klar, daß eine Abspeicherung der übermittelten Einzelangaben in Dateien für andere als statistische Nutzung (z. B. Fortschreibung von Gebäude-, Arbeitsstätten- oder Gewerbedateien) unzulässig ist. Gleiches gilt auch für die Zusammenführung der übermittelten Datensätze mit anderen Einzelangaben, durch die ein Personenbezug wiederhergestellt wird.

Absatz 5 legt sowohl für die übermittelnde Stelle als auch für die Dienststelle, die Daten nach Absatz 1 erhält, diejenigen Protokollierungspflichten fest, die für eine sachgerechte Kontrolle – insbesondere auch seitens des Datenschutzbeauftragten – erforderlich sind.

Zu § 33 (Straftaten)

Der Inhalt der Strafvorschriften ist neu geordnet und in Relation zu den Ordnungswidrigkeiten neu strukturiert. Damit ist auch ein Effekt der „Entkriminalisierung" verbunden. Fehlverhalten im Zusammenhang mit der Verarbeitung personenbezogener Daten, unabhängig davon, ob es sich um eine datei- oder nichtdateimäßige Verarbeitung handelt, ist nach Absatz 1 nur dann strafbewehrt, wenn es sich um ein qualifiziertes Delikt handelt, der Täter also in Bereicherungs- oder Schädigungsabsicht vorgeht. Die in Satz 1 Nrn. 1 bis 3 sowie in Satz 2 aufgeführten Tatbestände sind den neuen Regelungen dieses Gesetzes angepaßt; die Strafandrohung entspricht der bisherigen Höhe in § 33 Absatz 2. Auch der Versuch soll in Zukunft strafbar sein (Satz 3).

Nach Absatz 2 finden die Strafnormen des Datenschutzgesetzes Nordrhein-Westfalen jedoch nur dann Anwendung, wenn die Tat nicht nach anderen Vorschriften, insbesondere des Bundesrechts, mit Strafe bedroht ist. Angesichts des strafrechtlichen Gehalts der Vorschrift kann das bisherige Antragserfordernis bzw. das Antragsrecht des Landesbeauftragten für den Datenschutz nach § 33 Absatz 3 allerdings nicht erhalten bleiben. Die neue Vorschrift wird damit Offizialdelikt.

Zu § 34 (Ordnungswidrigkeiten)

Mit der Regelung, die Strafandrohung – auch im Hinblick auf die nicht dateimäßige Datenverarbeitung – nur noch für bestimmte schwerwiegende Delikte aufrecht zu erhalten, muß allerdings der Bereich der Ordnungswidrigkeiten ausgeweitet werden, da es grundsätzlich nicht im öffentlichen Interesse liegen kann, vorsätzliches Fehlverhalten im Umgang mit personenbezogenen Daten ohne Sanktion zu lassen. Die neue Vorschrift gilt in gleicher Weise für die formatierte wie die konventionelle Datenverarbeitung. Die in § 33 angepaßte und damit erheblich erweiterte Vorschrift enthält in Absatz 1 auch die bisher in § 33 Absatz 1 und § 34 enthaltenen Tatbestände.

Absatz 2 entspricht dem bisherigen § 34 Absatz 2.

Absatz 3 ersetzt die Verordnung über die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Datenschutzgesetz Nordrhein-Westfalen vom 25. November 1980 (GV. NW. S. 1049).

Zu § 35 (Übergangsvorschriften)

Die Vorschrift stellt in Absatz 1 klar, daß die Verpflichtung der speichernden Stelle zur Berichtigung, Sperrung oder Löschung personenbezogener Daten in Akten nach § 19 übergangsweise nur in den Fällen in Betracht kommt, in denen sich dies aus gegebenem Anlaß als notwendig herausstellt. Eine generelle Überprüfung vorhandener Aktenbestände von Amts wegen kann nicht verlangt werden.

Bis zu einer bereichsspezifischen Regelung durch Novellierung des Strafvollzugsgesetzes, die für die nächste Legislaturperiode des Bundestages vorgesehen ist, wird der Gesetzentwurf grundsätzlich auch für den Justizvollzug gelten. Das ist hinnehmbar, sofern die in § 18 angesprochenen Rechte in Absatz 2 begrenzt werden. Diese Begrenzung ist unverzichtbar. Eigenart und soziale Situation der Betroffenen im Justizvollzug lassen anderenfalls eine Fülle sachwidriger oder gar schikanöser Anträge erwarten. Durch deren – zeitraubende – Bearbeitung würde die Wahrnehmung vorrangiger Vollzugsaufgaben unerträglich beeinträchtigt.

Die bisherigen Vorschriften:

§ 35 (Übergangsvorschrift), § 36 (Meldebehörden), §§ 37 und 40 (Weitergeltende Vorschriften und haushaltsrechtliche Ermächtigungen) sowie § 41 (Inkrafttreten) sind mit der Neufassung des Gesetzes aufgehoben.

Zu Artikel 2

Aufhebung der Datenschutzveröffentlichungsverordnung NW

Die Aufhebung der Datenschutzveröffentlichungsverordnung folgt aus der Streichung des § 15 DSG a. F. über die Veröffentlichungspflicht.

Zu Artikel 3

Gesetz zur Änderung des Verwaltungsverfahrensgesetzes NW

A Allgemeines

Durch die Einbeziehung personenbezogener Datenverarbeitung in und aus Akten in den Anwendungsbereich des Datenschutzgesetzes wird dem Recht des Betroffenen auf informationelle Selbstbestimmung auch im Anwendungsbereich des Verwaltungsverfahrensgesetzes in umfassender Weise Rechnung getragen. Auf Grund dieser neuen Konzeption werden gesonderte Regelungen über die Verarbeitung personenbezogener Daten für das Verwaltungsverfahrensgesetz weitestgehend entbehrlich; nur soweit das Verwaltungsverfahren Besonderheiten aufweist, bleibt Raum für eine abweichende Regelung. Die für das Verwaltungsverfahrensgesetz vorgesehenen Ergänzungen haben deshalb im wesentlichen klarstellende Funktion; vor allem stellen sie den Vorrang des Datenschutzgesetzes bei der Verarbeitung personenbezogener Daten auch im Verwaltungsverfahren sicher. Im Besonderen werden die im Verwaltungsverfahrensgesetz niedergelegten Amtshilfe- und Amtsermittlungsgrundsätze (§§ 4, 24 Abs. 1, 26 Abs. 1 Verwaltungsverfahrensgesetz NW) einer verstärkten Zweckbindung nach Maßgabe des Datenschutzgesetzes (§§ 12 bis 14 DSG NW) unterworfen, soweit nicht bereichsspezifische und deshalb vorrangige Datenschutzregelungen bestehen.

B Im einzelnen

Zu Nr. 1 (§ 3a neu) und Nr. 3 (Fortfall des bisherigen § 30)

Der neue § 3a ersetzt die bisherige, auf das Verwaltungsverfahren im Sinne des § 9 VwVfG NW beschränkte Regelung des § 30 VwVfG. § 3a stellt durch eine inhaltliche Erweiterung die Verbindung zu den für die datenschutzrechtliche Beurteilung von Datenübermittlungen maßgeblichen Vorschriften des Datenschutzgesetzes her. Soweit das Verwaltungsverfahrensgesetz für die Akteneinsicht in einem Verwaltungsverfahren Beteiligter Besonderheiten aufweist, bleiben diese erhalten (§ 18 Absatz 2 Satz 2 DSG NW).

Zu Nr. 2a (§ 26 Abs. 1 Satz 1)

Durch den in § 26 Abs. 1 Satz 1 eingefügten Hinweis auf die neue Geheimhaltungsvorschrift des § 3a wird deutlich gemacht, daß § 26 Abs. 1 allein keine Befugnisnorm für die Erhebung personenbezogener Daten durch eine Behörde bei einer anderen Behörde darstellt, sondern eine solche Datenerhebung nur nach Maßgabe der einschlägigen datenschutzrechtlichen Bestimmungen zuläßt.

Zu Nr. 2b (§ 26 Abs. 2 Sätze 3 und 4)

Durch die Ergänzung in Satz 3 wird klargestellt, daß entsprechend den Ausführungen des Bundesverfassungsgerichts zur zwangsweisen Erhebung personenbezogener Daten der Betroffene zu einer Offenbarung personenbezogener Daten gegenüber der Behörde nur verpflichtet ist, soweit dies gesetzlich geregelt ist. Satz 4 trägt den Ausführungen des Bundesverfassungsgerichts im Volkszählungsurteil zum Schutz vor Selbstbezichtung als Grenze der Erhebungsermächtigung Rechnung (vgl. BVerfG 65, 1 [46]).

Zu Artikel 4

Gesetz zur Änderung des Meldegesetzes NW

A Allgemeines

Die für die Änderung des Datenschutzgesetzes Nordrhein-Westfalen maßgebenden grundsätzlichen Erwägungen, insbesondere die Weiterentwicklung des daten- und persönlichkeitsrechtlichen Schutzes des Bürgers unter Beücksichtigung des Urteils des Bundesverfassungsgerichts vom 15. 12. 1983 zum Volkszählungsgesetz 1983, sind auch für die Änderung des Meldegesetzes bestimmend. Dies gilt vornehmlich für den Wegfall der Speicherung der Daten „Beruf" und „Seriennummer des Personalausweises und des Passes" im Melderegister sowie für die Einführung eines Widerspruchsrechts des Bürgers gegenüber der Melderegisterauskunft an Adreßbuchverlage.

Zwar hat es der Bundesgesetzgeber im Zuge des Gesetzgebungsverfahrens zum Melderechtsrahmengesetz vom 16. August 1980 (BGBl. I S. 1429) den Bundesländern freigestellt, in ihren Meldegesetzen auch das Datum „Beruf" zur Speicherung in den Melderegistern zuzulassen (Bundestags-Drucksache 8/3825, S. 36 zu Nr. 5). Von einer solchen Regelung haben jedoch nicht alle Bundesländer Gebrauch gemacht. Ausschlaggebend dafür war letztlich, daß dieses Datum im Melderegister nicht aktuell gehalten werden und somit zu einer vor allem für den Betroffenen oftmals nachteiligen Unrichtigkeit des Melderegisters führen kann. Gleichwohl ist die Speicherung des Datums „Beruf" im Meldegesetz NW zugelassen worden, da sie im Interesse des Landes z. B. für die Erfassung der sog. „Medizinalpersonen" sowie für die

Berufung von Schöffen und Wahlvorständen geboten erschien (Landtags-Drucksache 9/1220, S. 36/37). Eine allgemeine Erhebung und Speicherung des Datums „Beruf" ist jedoch wegen der „informationellen Selbstbestimmung" des Bürges über seine personenbezogenen Daten nicht mehr zu begründen. Die vorliegende Novelle des Meldegesetzes NW beschränkt sich deshalb auf die Speicherung des Datums „Berufsausübung im Gesundheitswesen".

Mit der Streichung auch des Datums „Seriennummer des Pesonalausweises und des Passes" (§ 3 Absatz 2 Nr. 8 MG NW) wird der Novellierung des Bundespersonalausweisgesetzes und des Paßgesetzes Rechnung getragen. Auch insoweit hat zwar der Bundesgesetzgeber im Zuge des Gesetzgebungsverfahrens zum Melderechtsrahmengesetz die Speicherung dieses Datums im Melderegister, die in jenem Gesetz nicht besonders normiert ist, den Bundesländern für die Erfüllung von Landesaufgaben freigestellt (vgl. Bundestags- Drucksache 8/4333, S. 3 zu § 2 Abs. 1 Nr. 15). Für die Zukunft bestimmen nunmehr jedoch § 3 Abs. 4 Satz 3 des Gesetzes über Personalausweise (BGBl. I 1986 S. 548) und § 16 Abs. 4 Satz 3 des Paßgesetzes (BGBl. I 1986 S. 537), daß die Seriennummer des Personalausweises und des Passes ab 1. September 1991 nicht mehr im Melderegister gespeichert werden darf.

B Im einzelnen

Zu Nr. 1 Buchstabe a)

Die Überwachung der Wehr- oder Zivildienstpflicht liegt ausschließlich in der Zuständigkeit der Kreiswehrersatzämter bzw. des Bundesamtes für den Zivildienst. Gemäß § 24 Absatz 9 Wehrpflichtgesetz in der Fassung der Bekanntmachung vom 13. Juni 1986 (BGBl. I S. 879) und § 23 Absatz 3 Zivildienstgesetz – ZDG – in der Fassung der Bekanntmachung vom 31. Juli 1986 (BGBl. I S. 1205) teilt die Meldebehörde dem zuständigen Kreiswehrersatzamt zum Zwecke der Wehrüberwachung die in § 18 Absatz 1 des Melderechtsrahmengesetzes genannten Daten aller männlichen Deutschen zwischen dem vollendeten 18. und 32. Lebensjahr sowie spätere Änderungen dieser Daten mit; in gleicher Weise ist bei Wehrpflichtigen zu verfahren, von denen der Meldebehörde durch Mitteilung der Wehrersatzbehörde bekannt ist, daß sie auch nach Vollendung des 32. Lebensjahres der Wehrüberwachung unterliegen. Die Wehrersatzbehörde ihrerseits teilt dem Bundesamt für den Zivildienst die ihr von den Meldebehörden nach § 24 Abs. 9 Wehrpflichtgesetz übermittelten Personen, die nicht der Wehrpflicht unterliegen, zum Zwecke der Zivildienstüberwachung mit (§ 23 Abs. 3 Satz 1 ZDG).

Die technische und terminliche Abwicklung der regelmäßigen Datenübermittlung an die Kreiswehrersatzämter durch die Meldebehörden ist nunmehr durch § 2 der Zweiten Meldedaten-Übermittlungsverordnung des Bundes – 2. BMeldDÜV – vom 26. Juni 1984 (BGBl. I S. 810) geregelt.

In Anbetracht dieser nach Inkrafttreten des MG NW geschaffenen neuen Rechtslage ist eine Speicherung der Tatsache, daß ein Einwohner der Wehrüberwachung unterliegt, im Melderegister nicht mehr **generell** erforderlich; die Speicherung der Tatsache, daß ein Einwohner der Zivildienstüberwachung unterliegt, ist **insgesamt** entbehrlich.

Lediglich für diejenigen Wehrpflichtigen, von denen die Wehrersatzbehörde der Meldebehörde mitteilt, daß sie auch nach Vollendung des 32. Lebensjahres der Wehrüberwachung unterliegen, bedarf es noch einer Speicherung dieser Tatsache im Melderegister, damit die Meldebehörde auch für diesen Personenkreis den Mitteilungsdienst gegenüber dem zuständigen Kreiswehrersatzamt wahrnehmen kann.

Zu Nr. 1 Buchstabe b)

Das Erfordernis für die Speicherung des Datums „Berufsausübung im Gesundheitswesen" im Melderegister folgt aus der als Landesrecht fortgeltenden Dritten Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens vom 30. März 1935 (RGS. NW. S. 7/GV. NW. 1970 S. 18).

Nach dieser Durchführungsverordnung führt das Gesundheitsamt Listen über diejenigen Personen, die in seinem Bezirk selbständig oder in abhängiger Stellung Behandlung, Pflege oder gesundheitliche Fürsorge am Menschen ausüben, die Leichenschau betätigen oder die Entkeimung von Wohnungen und Gegenständen wahrnehmen. Das **Melde**register ist die **Grundlage** dieser Listenführung. Das Gesundheitsamt erhält von den An- und Abmeldungen rechtzeitig Kenntnis und ist verpflichtet, etwaige Ergänzungen anzufordern (§ 1 der o. a. Durchführungsverordnung).

Die regelmäßigen Datenübermittlungen der Meldebehörden an das Gesundheitsamt dienen u. a.

1. der Prüfung der Berechtigung der Berufsausübung (§ 1 Abs. 1 und § 2 a. a. O.),
2. der Überwachung der rechtmäßigen Verwendung einer Berufsbezeichnung (§ 20 Abs. 1 Satz 1 a. a. O.),

3. der Aufsicht (Gesundheitsaufsicht) über die Berufstätigkeit nach § 20 Abs. 1 Satz 2 und 3 a.a.O. sowie
4. der Zurücknahme einer staatlichen Anerkennung zur Ausübung des Berufs oder zur Führung einer bestimmten Berufsbezeichnung (§ 20 Abs. 2 a.a.O.).

Eine der wesentlichsten Aufgaben des Gesundheitsamtes, nämlich die Beobachtung der gesundheitlichen Lage der Bevölkerung und die Einleitung der erforderlichen Maßnahmen, kann nur dann erfüllt werden, wenn dem Gesundheitsamt entsprechende Daten über das Melderegister zugänglich sind.

Diesem Erfordernis trägt bereits § 4 der Ersten Verordnung über die Zulassung der regelmäßigen Datenübermittlung von Meldebehörden an andere Behörden oder sonstige öffentliche Stellen (1. MeldDÜV NW) vom 20. 6. 1983 – GV. NW. S. 221 – Rechnung, der die Datenübermittlung für Zwecke der Gesundheitsaufsicht durch die Meldebehörden an das Gesundheitsamt für ganz bestimmte Gruppen der Medizinalberufe im einzelnen zuläßt.

Im übrigen entspricht die in diesem Punkte vorgesehene Änderung des Meldegesetzes NW der Regelung in den bereits erlassenen Meldegesetzen der Länder Hamburg, Niedersachsen und Saarland.

Zu Nr. 1 Buchstabe c) und Nrn. 2 und 4

Durch die ersatzlose Streichung von § 3 Absatz 2 Nr. 8 MG NW i.V.m. Artikel 5 (Inkrafttreten) wird entsprechend dem Bundesrecht die Speicherung der Seriennummer des Personalausweises und des Passes im Melderegister nur noch befristet zugelassen. Ab 1. 9. 1991 ist eine Speicherung der Seriennummer des Personalausweises und des Passes im Melderegister nicht mehr zulässig. Hieraus ergeben sich Änderungen in § 11 Abs. 2 Satz 2 (s. Nr. 2) und in § 18 Abs. 1 Satz 1 (s. Nr. 4).

Zu Nr. 3

Die Vorschrift des § 11 Abs. 3 Satz 2 in der derzeitigen Fassung des Meldegesetzes NW führt dazu, daß aus den in die besonders gesicherte Aufbewahrung überführten Daten eines Einwohners weder dem Kirchlichen Suchdienst mit seinen Heimatortskarteien noch dem Suchdienst des Deutschen Roten Kreuzes Auskünfte aus dem Melderegister gegeben werden können über Personen, die seit mehr als fünf Jahren den Einzugsbereich der Meldebehörde verlassen haben oder verstorben sind. Beide Institutionen weisen demgegenüber darauf hin, daß es im Auftrage des Bundes und auf Grund von Vereinbarungen mit dem Bund, auf deren Grundlage sie noch heute tätig sind, ihre Aufgabe ist, nach Vermißten und Verschollenen des 2. Weltkrieges zu forschen sowie im Rahmen des Kindersuchdienstes das Schicksal verschollener Kinder aufzuklären. Die Wahrnehmung dieser Aufgaben werde ihnen durch die erwähnte Vorschrift des MG NW außerordentlich erschwert, ja praktisch sogar unmöglich gemacht, wenn ihnen eine Auskunft über den Wohnungsnachweis sowie über den Sterbetag und -ort einer im Melderegister erfaßten gesuchten Person verwehrt bleibt.

Im Prinzip ist diese Frage nicht nur allein für die Tätigkeit der Suchdienste von Belang, sondern auch dann von allgemeiner Bedeutung, wenn z. B. allernächste Angehörige nach dem ihnen unbekannten letzten Wohnort sowie dem Sterbetag und -ort ihrer Verwandten nachforschen. Eine derartige – aus humanitären Gründen als berechtigt anzuerkennende und datenschutzrechtlich nicht zu beanstandende, auf eng begrenzte Daten beschränkte – Melderegisterauskunft soll durch die beabsichtigte Gesetzesänderung ermöglicht werden. Gleiche Ausnahmebestimmungen enthalten die Meldegesetze der Länder Bayern, Hamburg und Schleswig-Holstein.

Zu Nr. 5

Die Streichung ist Folge der Änderung des Melderechtsrahmengesetzes durch Art. 5 des Gesetzes zur Änderung des Wehrrechts und des Zivildienstrechts vom 24. Februar 1983 – BGBl. I S. 179 –. Danach ist im Rahmen des **Rückmeldeverfahrens** nach § 17 Abs. 1 MRRG die Unterrichtung der Meldebehörde der neuen Wohnung durch die bisher zuständige Meldebehörde über die Tatsache, daß ein Einwohner der Wehr- oder Zivildienstüberwachung unterliegt, entfallen. Für eine davon abweichende landesrechtliche Regelung im MG NW, die nach § 17 Abs. 1 Satz 3 MRRG zulässig wäre, besteht kein Anlaß.

Zu Nr. 6 Buchstabe a)

Folgeänderungen zu Nr. 1 Buchstaben b) und c).

Eine Übermittlung des Datums „Berufsausübung im Gesundheitswesen" (§ 3 Absatz 2 Nr. 7 neu) sowie – ab 1. September 1991 – der Seriennummer des Personalausweises und des Passes an die in § 31 Absatz 3 genannten Sicherheitsbehörden entfällt.

Zu Nr. 6 Buchstabe b)

Die Einfügung ist erforderlich, da andernfalls nach der Streichung der Nr. 7 in § 31 Abs. 1 Satz 2 eine Ermächtigungsgrundlage für die regelmäßige Datenübermittlung nach § 4 der MeldDÜV NW für die sog. Medizinalpersonen fehlen würde (vgl. im übrigen oben zu Nr. 1 Buchstabe b).

Zu Nr. 7 Buchstaben a) und b)

Folgeänderung zu Nr. 1 Buchstabe b).

Zu Nr. 8

Mit Ausnahme des Meldegesetzes NW enthalten alle bisher von den Bundesländern erlassenen Meldegesetze ein Widerspruchsrecht des betroffenen Einwohners gegenüber der Melderegisterauskunft an Adreßbuchverlage. Dieses Widerspruchsrecht wird nunmehr auch im Meldegesetz NW eingeführt.

Zu Nr. 9

Das Bundesverfassungsgericht hat in seinem Urteil vom 15. 12. 1983 zum Volkszählungsgesetz 1983 die Kombination einer Volkszählung für statistische Zwecke mit einem Melderegisterabgleich für unzulässig erklärt.

§ 40 MG NW ist daher schon jetzt obsolet und somit zu streichen.

Zu Nr. 10

§ 41 MG NW ist wegen Zeitablaufs seiner Regelung zu streichen.

Zu Artikel 5

Gesetz zur Änderung des Gesetzes über den „Westdeutschen Rundfunk Köln"

Die Ergänzung des § 52 Absatz 1 Satz 1 des WDR-Gesetzes vom 19. März 1985 (GV. NW. S. 237) stellt – entsprechend der bisherigen Regelung in § 32 Absatz 1 Nr. 2 DSG NW – klar, daß die Vorschriften des Zweiten Teils des Datenschutzgesetzes (Art. 1) auf den Westdeutschen Rundfunk Köln keine Anwendung finden.

Zu Artikel 6

Neubekanntmachungsvorschrift

Der Artikel enthält die vor allem im Hinblick auf die Artikel 3 und 4 dieses Entwurfs erforderliche Ermächtigung zur Neubekanntmachung.

Zu Artikel 7

Inkrafttreten

Im Hinblick auf Artikel 1, § 34 Absatz 3 wird die Verordnung über die Zuständigkeit für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem DSG NW vom 25. 11. 1980 (GV. NW. S. 1049) aufgehoben. Die bisherigen §§ 38 und 39 des DSG bleiben trotz der Aufhebung des Datenschutzgesetzes in Kraft. Die einzeln aufgeführten Änderungen zu Artikel 4 treten erst mit dem 1. 9. 1991 in Kraft; insoweit wird auf die allgemeine Begründung zu Artikel 4 Bezug genommen.