

# **Gesetz zum Schutz des Bürgers beim Umgang mit seinen Daten (Landesdatenschutzgesetz von Mecklenburg-Vorpommern - DSG MV -)**

Vom 24. Juli 1992 (GVOBl. M-V S. 487), in Kraft am 15. August 1992, geändert durch Artikel 2 des Gesetzes vom 7. Juli 1997 (GVOBl. M-V S. 282), in Kraft am 24. Juli 1997, GS Meckl.-Vorp. Gl. Nr. 204-1

## **Der Landtag hat folgendes Gesetz beschlossen:**

Inhaltsübersicht

### **Abschnitt I Grundsatzregelungen**

- § 1 Zweck
- § 2 Anwendungsbereich
- § 3 Begriffsbestimmungen
- § 4 Umgang mit personenbezogenen Daten im Auftrag
- § 5 Datengeheimnis

### **Abschnitt II Umgang mit personenbezogenen Daten**

- § 6 Grundsatz
- § 7 Einwilligung
- § 8 Erheben
- § 9 Nutzen
- § 10 Verarbeiten
- § 11 Berichtigen, Sperren, Löschen
- § 12 Übermittlung an öffentliche Stellen
- § 13 Übermittlung an nicht-öffentliche Stellen
- § 14 Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes
- § 15 Automatisierte Abrufverfahren
- § 16 Dateibeschreibung und Geräteverzeichnis
- § 17 Technisch-organisatorische Maßnahmen
- § 18 Pflicht zur gegenseitigen Benachrichtigung
- § 19 Pflicht zur Benachrichtigung Betroffener

### **Abschnitt III Rechte des Betroffenen**

- § 20 Auskunft
- § 21 Sperrung durch den Betroffenen
- § 22 Anrufung des Landesbeauftragten für den Datenschutz
- § 23 Schadensersatz
- § 24 Unabdingbarkeit der Rechte Betroffener

### **Abschnitt IV Der Landesbeauftragte für den Datenschutz**

- § 25 Berufung und Rechtsstellung
- § 26 Kontrolle
- § 27 Unterstützung
- § 28 Beanstandungen
- § 29 Weitere Aufgaben

## **Abschnitt V Besondere Regelungen**

§ 30 Verarbeitung und Nutzung personenbezogener Daten zu wissenschaftlichen Zwecken

§ 31 Umgang mit personenbezogenen Daten bei Dienst- und Arbeitsverhältnissen

§ 32 Öffentliche Auszeichnungen

## **Abschnitt VI Strafvorschriften**

§ 33 Straftaten

## **Abschnitt VII Übergangsvorschriften**

§ 34 Zuständigkeit für personenbezogene Daten ehemaliger Einrichtungen

§ 35 Zulässige Nutzung und Zweckbestimmung der Speicherung personenbezogener Daten ehemaliger Einrichtungen

§ 36 Sperrung personenbezogener Daten ehemaliger Einrichtungen

§ 37 Inkrafttreten

## **Abschnitt I**

### **Grundsatzregelungen**

#### § 1 Zweck

Zweck dieses Gesetzes ist es, das Recht des einzelnen zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

#### § 2 Anwendungsbereich

(1) Dieses Gesetz gilt für Behörden und öffentlich-rechtlich organisierte Einrichtungen und Stellen des Landes, der Gemeinden, der Ämter, der Landkreise sowie für sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts und deren Vereinigungen ungeachtet ihrer Rechtsform (öffentliche Stellen).

(2) Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Verwendung gelöscht werden, sowie für Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen und alsbald vernichtet werden, gelten nur die §§ 5 und 17 sowie die §§ 25 bis 29. Diese Daten sind vor dem Zugriff Unbefugter zu schützen.

(3) Soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor. Für die Gerichte sowie für die Behörden der Staatsanwaltschaft gilt dieses Gesetz nur, soweit sie Verwaltungsaufgaben wahrnehmen. Darüber hinaus gelten für die Behörden der Staatsanwaltschaft, soweit sie keine Verwaltungsaufgaben wahrnehmen, die §§ 16, 22, 25 bis 29, 31 und 32 sowie die §§ 34 bis 36; die §§ 20 und 21 finden keine Anwendung.

(4) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur die §§ 16, 22, 25 bis 29, 31 und 32 sowie die §§ 34 bis 36. Mit Ausnahme der Vorschriften über die Meldepflichten und die Aufsichtsbehörde (§§ 32 und 38) sind im übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der §§ 43 und 44 anwendbar.

(5) Für Begnadigungsverfahren findet dieses Gesetz keine Anwendung.

#### § 3 Begriffsbestimmungen

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

(2) Eine Datei ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren verarbeitet und ausgewertet werden kann (automatisierte Datei), oder

2. jede sonstige Sammlung gleichartig aufgebauter personenbezogener Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe oder Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Umgang mit Daten ist jede Form ihrer Erhebung, Verarbeitung oder Nutzung ungeachtet der dabei angewendeten Verfahren.

(5) Erheben ist das Beschaffen von Daten.

(6) Nutzen ist die inhaltliche Auswertung und Verwendung von Daten.

(7) Verarbeiten ist das Speichern, Übermitteln, Verändern, Sperren, Anonymisieren oder Löschen von Daten. Im einzelnen ist

1. Speichern das Erfassen, Aufnehmen, Aufzeichnen oder Aufbewahren von Daten auf einem Datenträger; dazu zählt auch das Vervielfältigen,

2. Übermitteln das Bekanntgeben erhobener, gespeicherter oder durch sonstige Verarbeitung gewonnener Daten an Dritte in der Weise, daß die Daten durch die mit ihnen umgehende Stelle weitergegeben werden oder daß Dritte von der mit den Daten umgehenden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsehen oder abrufen,

3. Verändern das inhaltliche Umgestalten gespeicherter Daten,

4. Sperren das Verhindern des weiteren Umgangs mit gespeicherten Daten, ausgenommen in den Fällen, in denen dieses Gesetz den Umgang mit den Daten zuläßt,

5. Anonymisieren das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.

6. Löschen das dauerhafte Unkenntlichmachen gespeicherter Daten.

Darüber hinaus ist Verarbeiten jede Form des Umgangs mit Daten, die nicht in den Vorschriften der Absätze 5 und 6 aufgeführt ist.

(8) Eine mit Daten umgehende Stelle ist jede öffentliche Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder durch andere in ihrem Auftrag erheben, verarbeiten oder nutzen läßt.

(9) Dritter ist jede Person oder Stelle außerhalb der mit den personenbezogenen Daten umgehenden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen oder Stellen, die im Geltungsbereich des Grundgesetzes mit personenbezogenen Daten im Auftrag umgehen.

(10) Stellen innerhalb des öffentlichen Bereichs sind öffentliche Stellen nach § 2 Abs. 1 dieses Gesetzes sowie öffentliche Stellen des Bundes und der anderen Länder nach § 2 des Bundesdatenschutzgesetzes.

## § 4

### Umgang mit personenbezogenen Daten im Auftrag

(1) Wird mit personenbezogenen Daten durch andere Personen oder Stellen im Auftrag einer öffentlichen Stelle umgegangen, so bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 20, 21 und 23 genannten Rechte sind ihm gegenüber geltend zu machen. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die Gewährleistung der nach § 17 notwendigen technisch-organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Art und der Umfang des Umgangs mit personenbezogenen Daten sowie erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

(2) Der Auftragnehmer darf mit den personenbezogenen Daten nur im Rahmen der Weisungen des Auftraggebers umgehen. Ist der Auftragnehmer der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder eine andere Vorschrift über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, sicherzustellen, daß der Auftragnehmer die Vorschriften dieses Gesetzes befolgt und sich der Kontrolle des Landesbeauftragten für den Datenschutz nach Maßgabe der §§ 26 und 27 unterwirft. Der Auftraggeber hat den Landesbeauftragten für den Datenschutz über die Beauftragung zu informieren.

## § 5

### Datengeheimnis

Denjenigen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es während und nach Beendigung ihrer Tätigkeit untersagt, mit diesen Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck umzugehen (Datengeheimnis). Diese Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz in geeigneter Weise zu unterrichten und bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

## **Abschnitt II**

### **Umgang mit personenbezogenen Daten**

#### § 6 Grundsatz

Der Umgang mit personenbezogenen Daten ist nur zulässig, soweit

1. die Vorschriften dieses Gesetzes ihn zulassen,
2. eine andere Rechtsvorschrift ihn erlaubt oder zwingend voraussetzt oder
3. der Betroffene eingewilligt hat.

#### § 7 Einwilligung

Die Einwilligung des Betroffenen bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich eingeholt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild des Schriftstücks hervorzuheben. Der Betroffene ist in geeigneter Weise über die Bedeutung und Tragweite der Einwilligung, insbesondere über die Art und den Umfang der Erhebung, Verarbeitung und Nutzung sowie über Empfänger beabsichtigter Übermittlungen von Daten, aufzuklären. Die Anschrift der mit den Daten umgehenden Stelle ist ihm mitzuteilen. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.

#### § 8 Erheben

(1) Das Erheben personenbezogener Daten ist zulässig, wenn deren Kenntnis zur rechtmäßigen Erfüllung einer in der Zuständigkeit der erhebenden Stelle liegenden Aufgabe erforderlich ist, der Zweck der Erhebung hinreichend bestimmt ist und die Daten ohne Verstoß gegen Rechtsvorschriften offenbart werden können.

(2) Personenbezogene Daten sind beim Betroffenen und mit seiner Kenntnis zu erheben, es sei denn, daß eine Rechtsvorschrift eine andere Art der Erhebung erlaubt oder zwingend voraussetzt oder daß der Betroffene in eine andere Art der Erhebung eingewilligt hat.

(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist er in geeigneter Weise über den Zweck der Erhebung, die Art und den Umfang der Verarbeitung und Nutzung sowie über Empfänger beabsichtigter Übermittlungen der Daten aufzuklären. Die Anschrift der mit den Daten umgehenden Stelle ist ihm mitzuteilen. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

(4) Werden personenbezogene Daten nicht beim Betroffenen, sondern bei anderen Personen sowie bei nicht-öffentlichen Stellen aufgrund einer Rechtsvorschrift, die zur Auskunft verpflichtet, erhoben, so sind diese auf die Rechtsgrundlage, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen. Der Betroffene ist in geeigneter Weise über die Erhebung entsprechend Absatz 3 Satz 1 und 2 zu unterrichten, wenn und soweit dadurch die Erfüllung der Aufgabe der erhebenden Stelle nicht mehr gefährdet ist.

## § 9

### Nutzen

(1) Das Nutzen personenbezogener Daten ist zulässig, wenn und soweit es zur Erfüllung einer in der Zuständigkeit der nutzenden Stelle liegenden Aufgabe erforderlich ist.

(2) Personenbezogene Daten dürfen nur für den Zweck genutzt werden, für den sie erhoben worden sind. Ist keine Erhebung vorausgegangen, so dürfen die Daten für den Zweck genutzt werden, für den sie bei ihrer erstmaligen Speicherung bestimmt wurden. Empfänger übermittelter Daten dürfen diese für den bei ihrer Übermittlung bestimmten Zweck nutzen.

(3) Das Nutzen personenbezogener Daten zu anderen Zwecken ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, daß es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
7. es zur Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand

erreicht werden kann.

Der andere Zweck muß hinreichend bestimmt sein. Besondere Amts- oder Berufsgeheimnisse bleiben unberührt.

(4) Personenbezogene Daten, die für andere Zwecke erhoben oder erstmalig gespeichert worden sind, dürfen zu Zwecken der Ausübung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen in dem dafür erforderlichen Umfang genutzt werden. Der Zugriff auf personenbezogene Daten ist nur insoweit zulässig, als dieser für die Ausübung der Befugnisse nach Satz 1 unerlässlich oder unvermeidbar ist. Eine Nutzung personenbezogener Daten zu Ausbildungs- und Prüfungszwecken ist zulässig, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(5) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür genutzt werden dürften, wenn sie nicht gesperrt wären.

## § 10

### Verarbeiten

(1) Das Verarbeiten personenbezogener Daten ist zulässig, wenn es zur Erfüllung einer in der Zuständigkeit der verarbeitenden Stelle liegenden Aufgabe erforderlich ist. Die Inanspruchnahme Dritter ist zulässig; in diesem Fall gilt der § 4.

(2) Personenbezogene Daten dürfen nur zu Zwecken ihrer zulässigen Nutzung nach § 9 und in dem dafür notwendigen Umfang gespeichert, übermittelt oder verändert werden.

(3) Sind die für einen zulässigen Nutzungszweck notwendigen Daten mit anderen Daten oder mit gesperrten Daten in Akten oder nicht-automatisierten Dateien derart verbunden, daß eine Trennung der Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, so ist auch eine Mitverarbeitung dieser Daten zulässig, sofern sie nicht Ändern oder Löschen ist. Eine Nutzung dieser Daten ist unzulässig. Im Falle der Übermittlung dieser Daten ist der Empfänger in geeigneter Weise auf das Nutzungsverbot hinzuweisen.

## § 11\*

### Berichtigen, Sperren und Löschen

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten in nicht-automatisierten Dateien oder Akten zu berichtigen, so soll in geeigneter Weise kenntlich gemacht werden, zu welchem Zeitpunkt und aus welchem Grunde sie unrichtig waren oder geworden sind. Personenbezogene Daten sind zu ergänzen, wenn der Zweck der Speicherung oder das berechtigte Interesse des Betroffenen dies erfordern.

(2) Personenbezogene Daten sind zu löschen, wenn

1. sie unrichtig sind und die mit den Daten umgehende Stelle keine Kenntnis der richtigen

Daten erlangen kann,

2. ihre Erhebung unzulässig war,

3. ihre Speicherung unzulässig ist oder

4. ihre Speicherung zur Erfüllung der in der Zuständigkeit der mit den Daten umgehenden Stelle liegenden Aufgabe nicht mehr erforderlich ist.

(3) An Stelle der Berichtigung oder Löschung tritt eine Sperrung, solange

1. einer Löschung nach Absatz 2 Nr. 4 Rechts- oder Verwaltungsvorschriften entgegenstehen,

2. Grund zur Annahme besteht, daß durch die Berichtigung oder Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden,

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder

4. es der Betroffene nach § 21 verlangt.

(4) Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Absatz 2 Nr. 4 nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Soweit hiernach eine Löschung nicht in Betracht kommt, sind die Daten zu sperren.

(5) Gesperrte Daten sind gesondert zu speichern. Ist dies nicht möglich, so sind die Daten mit einem entsprechenden Vermerk zu versehen. Gesperrte Daten dürfen über ihre Speicherung hinaus, außer zu Zwecken ihrer zulässigen Nutzung und in den Fällen des § 10 Abs. 3, nicht mehr verarbeitet werden. Gesperrte Daten dürfen vor Ablauf ihrer Sperrfrist nicht verändert oder gelöscht werden.

(6) Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, darf eine Löschung erst erfolgen, wenn das zuständige öffentliche Archiv die Übernahme abgelehnt oder über sie nicht fristgerecht entschieden hat.

---

\* § 11 Abs. 6 angefügt durch Artikel 2 des Gesetzes vom 7. Juli 1997.

## § 12

Übermittlung an Stellen innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Stellen innerhalb des öffentlichen Bereichs ist über § 10 hinaus zulässig, wenn die Nutzung der Daten zur Erfüllung einer in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich und nach § 9 zulässig ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungersuchen im Rahmen

der Aufgaben des Empfängers liegt, es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht.

(3) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 und 2 entsprechend, sofern sichergestellt ist, daß bei dem Empfänger ausreichend Datenschutzmaßnahmen getroffen werden. Die Feststellung trifft der Innenminister im Einvernehmen mit dem Landesbeauftragten für den Datenschutz.

### § 13

#### Übermittlung an Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs ist über § 10 hinaus zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. In diesem Falle unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung. Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

### § 14

#### Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen gilt § 13 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Verordnungen. Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen wird.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt werden.

### § 15

#### Automatisierte Abrufverfahren

(1) Ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte darf nur eingerichtet werden, wenn eine Rechtsvorschrift dies ausdrücklich zuläßt.

(2) Die Landesregierung wird ermächtigt, die Einrichtung automatisierter Abrufverfahren durch Rechtsverordnung einzuführen, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgabe der beteiligten Stellen angemessen ist. Der Landesbeauftragte für den Datenschutz ist vorher zu hören. In der

Rechtsverordnung sind die Datenempfänger, die Datenart und der Zweck des Abrufs festzulegen. Darüber hinaus sind Maßnahmen zur Datensicherung und zur Kontrolle vorzusehen, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

## § 16

### Dateibeschriftung und Geräteverzeichnis

(1) Die speichernde Stelle ist verpflichtet, in einer Beschreibung jeder automatisierten Datei festzulegen:

1. die Bezeichnung der Datei,
2. die Art der gespeicherten Daten,
3. die Art und den Umfang der Nutzung der Daten,
4. den Kreis der Betroffenen,
5. die Art der regelmäßig übermittelten Daten und deren Empfänger,
6. die Art der regelmäßig empfangenen Daten und deren Herkunft,
7. bestehende Fristen für die Sperrung oder Löschung der Daten,
8. die technisch-organisatorischen Maßnahmen nach § 17,
9. bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.

(2) Die speichernde Stelle ist verpflichtet, in einem Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, neben der Dateibeschriftung nach Absatz 1 festzulegen:

1. den Standort, den Typ und die Art der Geräte,
2. den Hersteller,
3. das verwendete Betriebssystem,
4. die verwendeten Programme.

(3) Die Dateibeschriftung und das Geräteverzeichnis sind laufend auf dem neuesten Stand zu halten. Sie sind dem Landesbeauftragten für den Datenschutz auf Anforderung zu übermitteln.

## § 17

### Technisch-organisatorische Maßnahmen

(1) Die mit personenbezogenen Daten umgehende und die in ihrem Auftrag tätige Stelle hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich und angemessen sind, um die Einhaltung der Vorschriften dieses Gesetzes und anderer

Vorschriften über den Datenschutz sicherzustellen und insbesondere die Wahrnehmung der Rechte nach §§ 20 und 21 durch den Betroffenen zu gewährleisten.

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

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, 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 personenbezogener Daten zu verhindern (Speicherkontrolle),
4. die Benutzung von Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte zu verhindern (Benutzerkontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen wann welche personenbezogenen Daten übermittelt worden sind (Übermittlungskontrolle),
7. zu gewährleisten, daß nachträglich überprüft 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 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 nicht-automatisierten Dateien oder Akten verarbeitet, sind Maßnahmen zu treffen, die je nach Art der Datenverarbeitung und der zu schützenden personenbezogenen Daten erforderlich sind, Kontrollen nach Absatz 2 Nr. 1, 2, 6, 9 und 10 zu gewährleisten.

## § 18

### Pflicht zur gegenseitigen Benachrichtigung

Werden durch eine mit personenbezogenen Daten umgehende Stelle unrichtige, unzulässig erhobene oder unzulässig gespeicherte Daten berichtigt, gesperrt oder

gelöscht, so benachrichtigt diese die anderen mit diesen Daten umgehenden Stellen, insbesondere die Empfänger von Übermittlungen. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßig hohen Aufwand erfordern würde und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

## § 19

### Pflicht zur Benachrichtigung Betroffener

Hat eine mit personenbezogenen Daten umgehende Stelle Grund zur Annahme oder Kenntnis, daß unrichtige, unzulässig erhobene oder unzulässig gespeicherte personenbezogene Daten bereits derart genutzt wurden, daß dem Betroffenen daraus ein Nachteil entstanden ist oder zu entstehen droht, so hat sie diesen unverzüglich zu benachrichtigen.

## **Abschnitt III**

### **Rechte des Betroffenen**

## § 20

### Auskunft

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und
2. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße 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 oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder dem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, daß er sich an den Landesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Landesbeauftragten für den Datenschutz an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zugestimmt hat.

(7) Die Auskunft ist unentgeltlich.

## § 21

### Sperrung durch den Betroffenen

(1) Der Betroffene hat das Recht, personenbezogene Daten sperren zu lassen, soweit er deren Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit nachweisen läßt.

(2) Der Betroffene hat das Recht, bis zur Klärung von Schadensersatzansprüchen unrichtige, unzulässig erhobene oder unzulässig gespeicherte Daten zu seiner Person, die bereits genutzt wurden, auf Antrag bei der mit den Daten umgehenden Stelle sperren zu lassen. Die Sperrung wird nach Ablauf von sechs Monaten vom Zeitpunkt des Sperrantrags an unwirksam, wenn durch den Betroffenen innerhalb dieses Zeitraums kein Schadensersatzanspruch gerichtlich geltend gemacht wurde.

## § 22

### Anrufung des Landesbeauftragten für den Datenschutz

Jeder hat das Recht, sich an den Landesbeauftragten für den Datenschutz zu wenden, wenn er annimmt, beim Umgang mit seinen personenbezogenen Daten durch eine der Kontrolle des Landesbeauftragten für den Datenschutz unterliegenden Stellen in seinen Rechten verletzt worden zu sein; Beschäftigte öffentlicher Stellen können sich dabei ohne Einhaltung des Dienstwegs an den Landesbeauftragten für den Datenschutz wenden.

## § 23

### Schadensersatz

(1) Fügt eine mit personenbezogenen Daten umgehende Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierten Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einer Höhe von zweihundertfünfzigtausend Deutsche Mark begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von zweihundertfünfzigtausend Deutsche Mark übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer Datei mehrere mit den Daten umgehende Stellen beteiligt und ist der Geschädigte nicht in der Lage, die verursachende Stelle festzustellen, so haftet jede dieser Stellen.

(5) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(6) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§ \*254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(7) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verantwortlich ist, bleiben unberührt.

(8) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

## § 24

### Unabdingbarkeit der Rechte Betroffener

Die Rechte nach den §§ 20 bis 23 können auch durch die Einwilligung des Betroffenen nicht ausgeschlossen oder beschränkt werden.

## **Abschnitt IV**

### **Der Landesbeauftragte für den Datenschutz**

## § 25

### Berufung und Rechtsstellung

(1) Das Amt des Landesbeauftragten für den Datenschutz wird beim Präsidenten des Landtags eingerichtet.

(2) Der Landtag wählt ohne Aussprache den Landesbeauftragten für den Datenschutz mit mehr als der Hälfte seiner Mitglieder für die Dauer von sechs Jahren. Die Wiederwahl ist nur einmal zulässig. Vorschlagsberechtigt sind die Fraktionen des Landtags. Kommt vor Ablauf der Amtszeit eine Neuwahl nicht zustande, führt der Landesbeauftragte für den Datenschutz das Amt bis zur Neuwahl weiter.

(3) Der Präsident des Landtags ernennt den Landesbeauftragten für den Datenschutz zum Beamten auf Zeit.

(4) Der Landesbeauftragte für den Datenschutz bestellt einen Mitarbeiter zum Stellvertreter. Der Stellvertreter führt die Geschäfte, wenn der Landesbeauftragte für den Datenschutz an der Ausübung des Amtes verhindert ist.

(5) Vor Ablauf der Amtszeit kann der Landesbeauftragte nur mit einer Mehrheit von zwei Dritteln der Mitglieder des Landtags abberufen werden. Der Landesbeauftragte für den Datenschutz kann jederzeit die Entlassung verlangen.

(6) Der Landesbeauftragte für den Datenschutz ist in der Ausübung des Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Präsidenten des Landtags. Für die Erfüllung der Aufgaben ist die notwendige Personal- und Sachausstattung zur Verfügung zu stellen; die Mittel sind im Einzelplan des Landtags in einem gesonderten Kapitel auszuweisen.

(7) Die Mitarbeiter werden auf Vorschlag des Landesbeauftragten für den Datenschutz ernannt. Sie können nur im Einvernehmen mit ihm versetzt oder abgeordnet werden. Ihr Dienstvorgesetzter ist der Landesbeauftragte für den Datenschutz, an dessen Weisungen sie ausschließlich gebunden sind.

(8) Der Landesbeauftragte für den Datenschutz ist oberste Dienstbehörde im Sinne des § 96 der Strafprozeßordnung und oberste Aufsichtsbehörde im Sinne des § 99 der Verwaltungsgerichtsordnung. Er trifft die Entscheidungen über Aussagegenehmigungen für sich und die Mitarbeiter in eigener Verantwortung.

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

## § 26 Kontrolle

(1) Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen. Er kontrolliert die Einhaltung der Datenschutzvorschriften auch bei Stellen, die sich und soweit sie sich seiner Kontrolle unterworfen haben.

(2) Der Landesbeauftragte für den Datenschutz teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung der festgestellten Mängel beim Umgang mit personenbezogenen Daten, verbinden. § 28 bleibt unberührt.

## § 27 Unterstützung

(1) Die öffentlichen Stellen und diejenigen Stellen, die sich der Kontrolle des Landesbeauftragten für den Datenschutz unterworfen haben, sind verpflichtet, ihn und seine Beauftragten bei der Aufgabenerfüllung, namentlich bei der Durchführung von Kontrollen zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen zu gewähren, die in Zusammenhang des Umgangs mit personenbezogenen Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungssysteme und Programme,

2. jederzeit Zutritt zu allen Diensträumen zu gewähren.

(2) Die Rechte nach Absatz 1 dürfen nur vom Landesbeauftragten für den Datenschutz persönlich ausgeübt werden, wenn die zuständige oberste Landesbehörde im Einzelfall feststellt, daß die Sicherheit des Bundes oder eines Landes dies gebietet.

## § 28

### Beanstandungen

(1) Stellt der Landesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel beim Umgang mit personenbezogenen Daten fest, so beanstandet er dies

1. bei den Behörden des Landes gegenüber der zuständigen obersten Landesbehörde,

2. bei den Gemeinden, Ämtern und Landkreisen gegenüber dem verwaltungsleitenden Organ,

3. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In Fällen von Satz 1 Nr. 2 und 3 unterrichtet der Landesbeauftragte für den Datenschutz gleichzeitig auch die zuständige oberste Aufsichtsbehörde.

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

(3) 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 Satz 1 Nr. 2 und 3 genannten Stellen leiten der zuständigen obersten Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz zu.

(4) Der Landesbeauftragte für den Datenschutz kann nach pflichtgemäßem Ermessen Betroffene von Verstößen gegen die Vorschriften dieses Gesetzes oder andere Datenschutzvorschriften unterrichten.

## § 29

### Weitere Aufgaben

(1) Der Landesbeauftragte für den Datenschutz hat dem Landtag und der Landesregierung jeweils für zwei Kalenderjahre einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Die Landesregierung leitet dazu innerhalb von drei Monaten nach Vorlage dieses Berichts ihre Stellungnahme dem Landtag zu.

(2) Der Landesbeauftragte für den Datenschutz berät die obersten Landesbehörden sowie die sonstigen öffentlichen Stellen in Fragen des Datenschutzes. Dabei kann er Empfehlungen zur Verbesserung des Datenschutzes geben. Der Landtag und die Landesregierung können den Landesbeauftragten für den Datenschutz mit der Erstellung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen betrauen.

(3) Der Landesbeauftragte für den Datenschutz wirkt auf eine Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den für nicht-öffentlichen Stellen nach dem Bundesdatenschutzgesetz zuständigen Aufsichtsbehörden hin.

(4) Der Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit in angemessener Form zu Fragen des Datenschutzes.

(5) Der Landesbeauftragte für den Datenschutz beobachtet die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung, und ihre Auswirkungen auf die Arbeitsweise der öffentlichen Stellen. Zu diesem Zweck ist er über Verfahrensentwicklungen im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend zu unterrichten.

## **Abschnitt V**

### **Besondere Regelungen**

#### § 30

Verarbeitung und Nutzung personenbezogener Daten  
zu wissenschaftlichen Zwecken

(1) Personenbezogene Daten dürfen ohne Einwilligung des Betroffenen nur zu bestimmten Zwecken wissenschaftlicher Forschung genutzt werden, soweit

1. dessen schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Nutzung nicht beeinträchtigt werden oder

2. die zuständige oberste Aufsichtsbehörde festgestellt hat, daß das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

(2) Die Übermittlung personenbezogener Daten zum Zwecke wissenschaftlicher Forschung ist nur unter den Voraussetzungen des Absatzes 1 zulässig und bedarf der vorherigen Genehmigung der obersten Aufsichtsbehörde. Die Genehmigung muß den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und den Forschungszweck bezeichnen und ist dem Landesbeauftragten für den Datenschutz mitzuteilen.

(3) Die übermittelten personenbezogenen Daten dürfen ohne Einwilligung des Betroffenen nicht weiter übermittelt oder für einen anderen als den ursprünglichen Forschungszweck genutzt werden.

(4) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(5) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit und solange der Forschungszweck dies erfordert.

(6) Die wissenschaftliche Forschung betreibende Stelle darf personenbezogene Daten nur veröffentlichen, soweit

1. der Betroffene eingewilligt hat oder

2. dieses für die Darstellung von Forschungsergebnissen über die Ereignisse der Zeitgeschichte unerlässlich ist.

(7) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten an ihn nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Absätze 3 bis 6 einzuhalten und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

## § 31

Umgang mit personenbezogenen Daten bei Dienst- und Arbeitsverhältnissen

(1) Öffentliche Stellen dürfen mit Daten ihrer Beschäftigten nur umgehen, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung es vorsehen.

(2) Eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, wenn

1. der Betroffene eingewilligt hat,

2. eine Rechtsvorschrift dies vorsieht,

3. Art oder Zielsetzung der einem Beschäftigten übertragenen Aufgabe oder der Dienstverkehr es erfordert oder

4. der Empfänger ein rechtliches Interesse glaubhaft macht und der Betroffene vor der Übermittlung unterrichtet wurde und dieser nicht widersprochen hat.

(3) Die Übermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(4) Das Erheben medizinischer Daten aufgrund ärztlicher Untersuchungen zum Zwecke der Eingehung eines Dienst- oder Arbeitsverhältnisses ist nur zulässig, soweit dadurch die Eignung des Bewerbers hierfür festgestellt wird und er seine Einwilligung erteilt hat. Das

Erheben psychologischer Daten zur Eingehung eines Dienst- oder Arbeitsverhältnisses ist nur zulässig, soweit dies wegen der besonderen Anforderungen an die vorgesehene Tätigkeit erforderlich ist und der Bewerber hierzu seine Einwilligung erteilt hat. Der Dienstherr darf in der Regel nur das Ergebnis der Untersuchungen anfordern.

(5) Personenbezogene Daten, die zu Zwecken der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind zu löschen, sobald feststeht, daß ein Dienst- oder Arbeitsverhältnis nicht zustande kommt. Dies gilt nicht, wenn der Betroffene in die weitere Speicherung eingewilligt hat oder soweit Rechtsvorschriften einer Löschung entgegenstehen. Besteht Grund zu der Annahme, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden, ist er zu benachrichtigen. Soweit Rechtsvorschriften nicht entgegenstehen, sind personenbezogene Daten nach Beendigung eines Dienst- oder Arbeitsverhältnisses zu löschen, wenn diese nicht mehr benötigt werden.

(6) Beurteilungen und Personalentscheidungen dürfen nicht allein auf Informationen gestützt werden, die aus automatisierter Datenverarbeitung gewonnen werden; medizinische und psychologische Befunde von Beschäftigten oder Bewerbern dürfen vom Dienstherrn oder Arbeitgeber nicht automatisiert verarbeitet werden.

(7) Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 17 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

## § 32

### Öffentliche Auszeichnungen

(1) Zur Vorbereitung öffentlicher Auszeichnungen dürfen der Ministerpräsident, der Innenminister sowie die von dem Ministerpräsidenten besonders beauftragten Stellen die dazu erforderlichen personenbezogenen Daten auch ohne Kenntnis des Betroffenen erheben. Die Nutzung dieser Daten für andere Zwecke ist nur mit Einwilligung des Betroffenen zulässig.

(2) Auf Anforderung der in Absatz 1 genannten Stellen dürfen andere öffentliche Stellen die zur Vorbereitung der Auszeichnung erforderlichen Daten übermitteln.

(3) § 20 findet keine Anwendung.

## **Abschnitt VI Strafvorschriften**

### **§ 33 Straftaten**

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

1. speichert, verändert oder übermittelt,
2. zum Abruf mittels automatisierten Verfahrens bereithält oder
3. abrufen oder sich oder einem anderen aus Dateien verschafft,

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

(2) Ebenso wird bestraft, wer

1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,
2. entgegen § 13 Abs. 2 Satz 2 oder § 30 Abs. 4 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
3. entgegen § 30 Abs. 5 Satz 3 die in § 30 Abs. 5 Satz 2 bezeichneten Merkmale mit Einzelangaben zusammenführt.

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

(4) Die Tat wird nur auf Antrag verfolgt.

## **Abschnitt VII Übergangsvorschriften**

### **§ 34 Zuständigkeit für personenbezogene Daten ehemaliger Einrichtungen**

(1) Personenbezogene Daten ehemaliger Einrichtungen stehen derjenigen öffentlichen Stelle zu, auf die die Aufgaben dieser Einrichtungen übergegangen sind. Sie ist die verantwortliche speichernde Stelle. Ist eine Zuordnung der Daten nach Satz 1 nicht möglich, so bestimmt der Innenminister durch Verordnung die zuständige öffentliche Stelle.

(2) Personenbezogene Daten ehemaliger Einrichtungen sind personenbezogene Daten, die vor dem 3. Oktober 1990 von ehemaligen Einrichtungen nach ihrer Zweckbestimmung überwiegend für Verwaltungsaufgaben gespeichert waren, die nach dem Grundgesetz von

öffentlichen Stellen wahrzunehmen sind.

(3) Ehemalige Einrichtungen sind ehemalige staatliche Organe, Kombinate, Betriebe oder Einrichtungen der Deutschen Demokratischen Republik auf dem Gebiet des Landes Mecklenburg-Vorpommern.

#### § 35

Zulässige Nutzung und Zweckbestimmung der Speicherung personenbezogener Daten ehemaliger Einrichtungen

Die Nutzung personenbezogener Daten ehemaliger Einrichtungen ist zulässig, soweit ihre Kenntnis zur rechtmäßigen Erfüllung einer in der Zuständigkeit der speichernden Stelle liegenden Aufgabe erforderlich ist und die Art und der Umfang der weiteren Nutzung eindeutig bestimmt ist. Diese Daten gelten als für den nach Satz 1 bestimmten Zweck erstmalig gespeichert.

#### § 36

Sperrung personenbezogener Daten ehemaliger Einrichtungen

Personenbezogene Daten ehemaliger Einrichtungen, deren Nutzung nicht nach § 35 zulässig ist, sind zu sperren. Die Landesregierung regelt durch Verordnung den weiteren Umgang mit diesen Daten bis zum Inkrafttreten eines Landesarchivgesetzes.

#### § 37

Inkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Das vorstehende Gesetz wird hiermit verkündet.

Schwerin, den 24. Juli 1992

Für den Ministerpräsidenten  
Der Sozialminister  
Dr. Klaus Gollert

Der Innenminister  
Lothar Kupfer