SCHLESWIG-HOLSTEINISCHER LANDTAG
14. Wahlperiode

Drucksache 14/2258
24. 06. 99

Gesetzentwurf

der Landesregierung

Entwurf eines schleswig-holsteinischen Gesetzes zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz – LDSG –)

Federführend ist der Innenminister.

Die Landtagsdrucksachen sind fortlaufend und einzeln beim Verlag Schmidt & Klaunig, Ringstraße 19, 24114 Kiel, Tel. (0431) 6 60 64-0, Fax (0431) 6 60 64-24, zu beziehen.

Drucksache 14/2258

Gesetzentwurf der Landesregierung

Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen

A. Problem

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Abl. EG Nr. l.281 vom 23. Noemer 1995, S. 31) ist nach Art. 32 Abs. 1 in nationales Recht umzusetzen. Aus ihr ergibt sich ein weitreichender Änderungsbedarf auch für das Landesdatenschutzgesetz.

Die in der Richtlinie vorgesehene Umsetzungsfrist von drei Jahren ist am 24. Oktober 1998 abgelaufen. Daher besteht Handlungsbedarf.

B. Lösung

Die Richtlinie wird durch eine Neufassung des geltenden LDSG umgesetzt.

Über die Anpassung an die Richtlinie hinaus wird die Novellierung zum Anlaß genommen,

- auf Veränderungen der Technik datenschutzrechtlich zu reagieren (Regelung zu mobilen Datenverarbeitungssystemen wie z.B. Chipkarten),
- die Prinzipien der Datenvermeidung und Datensparsamkeit sowie der frühestmöglichen Anonymisierung und Pseudonymisierung stärker zu betonen,
- das Erfordernis eines Datenschutzes durch Technik zu normieren,
- ein Datenschutz-Audit einzuführen und
- die Serviceorientierung des Datenschutzes auszubauen.

Soweit möglich, werden die datenschutzrechtlichen Vorschriften und Verfahren vereinfacht und „entbürokratisiert".

C. Alternativen

Keine

D. Direkte Kosten und Verwaltungsaufwand

Direkte zusätzliche Kosten werden nicht entstehen.
Der Verwaltungsaufwand wird sich mit entsprechenden finanziellen Auswirkungen erhöhen durch zusätzliche Verpflichtungen, insbesondere im Zusammenhang mit der durch die EG-Richtlinie vorgeschriebenen Stärkung der Betroffenenrechte, und reduzieren durch die Vereinfachung bzw. den Wegfall bisher bestehender Melde- und Benachrichtigungspflichten sowie die Möglichkeit der gemeinsamen Nutzung automatisierter Verfahren durch mehrere Behörden.
Soweit öffentliche Stellen von der Möglichkeit Gebrauch machen, eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten zu bestellen, ergeben sich entsprechende Personalkosten. Diese werden zumindest teilweise kompensiert werden durch eingesparten Verwaltungsaufwand (Meldepflichten gegenüber der oder dem Landesbeauftragten für Datenschutz).

E. Federführung

Innenministerium des Landes Schleswig-Holstein

Entwurf eines Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (Landesdatenschutzgesetz - LDSG -)

Vom

Inhaltsübersicht:

Abschnitt III
Besondere Formen der Datenverarbeitung

Abschnitt IV
Besondere Zwecke der Datenverarbeitung

Abschnitt V
Rechte der Betroffenen

Der Landtag hat das folgende Gesetz beschlossen:

Abschnitt I
Allgemeine Grundsätze

§ 1
Gesetzeszweck

Zweck dieses Gesetzes ist es, bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen das Recht auf informationelle Selbstbestimmung zu wahren.

§ 2
Begriffsbestimmungen

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

(2) Datenverarbeitung ist die Verwendung personenbezogener Daten. Dabei ist

1. Erheben das Beschaffen von Daten,
2. Speichern das Aufbewahren von Daten auf Datenträgern,
3. Übermitteln das Weitergeben von Daten an Dritte oder der Abruf von zum Abruf bereitgehaltenen Daten durch Dritte,
4. Sperren das Untersagen weiterer Verarbeitung gespeicherter Daten,
5. Löschen das Unkenntlichmachen gespeicherter Daten,
6. Anonymisieren das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,
7. Pseudonymisieren das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,
8. Verschlüsseln das Verändern personenbezogener Daten derart, daß ohne Nutzung des Schlüssels die Kenntnisnahme vom Inhalt der Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist.

(3) Datenverarbeitende Stelle ist jede öffentliche Stelle im Sinne von § 3 Abs. 1, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt.

(4) Empfänger ist jede natürliche oder juristische Person, öffentliche oder nicht-öffentliche Stelle, die Daten erhält.

(5) Dritte oder Dritter ist jede natürliche oder juristische Person und öffentliche oder nicht-öffentliche Stelle außer

1. der datenverarbeitenden Stelle selbst,
2. der betroffenen Person,
3. der Auftragsdatenverarbeiterin oder dem Auftragsdatenverarbeiter und
4. den Personen, die unter der unmittelbaren Verantwortung der datenverarbeitenden Stelle oder der Auftragsdatenverarbeiterin oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

§ 3
Anwendungsbereich

(1) Dieses Gesetz gilt für öffentliche Stellen. Öffentliche Stellen im Sinne dieses Gesetzes sind

1. Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung,
2. Vereinigungen des privaten Rechts, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen und an der Vereinigung einem oder mehreren der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

(2) Soweit öffentlich-rechtliche, der Aufsicht des Landes unterstehende Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, gilt für sie von diesem Gesetz nur § 23; im übrigen gelten für sie die Vorschriften des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen. Für die Datenzentrale Schleswig-Holstein gelten die Vorschriften dieses Gesetzes.

(3) Soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor.

§ 4
Datenvermeidung und Datensparsamkeit, Datenschutzaudit

(1) Die datenverarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

(2) Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Verordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.

§ 5
Allgemeine Maßnahmen zur Datensicherheit

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere

1. Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren,
2. zu verhindern, daß personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können,
3. zu gewährleisten, daß die datenverarbeitende Person, der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann.

(2) Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach Änderungen durch die Leiterin oder den Leiter der datenverarbeitenden Stelle oder eine befugte Person freizugeben.

(3) Die Landesregierung regelt durch Verordnung die Anforderungen an das Sicherheitskonzept sowie die Freigabe automatisierter Verfahren und weitere Einzelheiten einer ordnungsgemäßen Datenverarbeitung der öffentlichen Stellen. Die oder der Landesbeauftragte für Datenschutz ist anzuhören.

§ 6
Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

(1) Automatisierte Verfahren sind so zu gestalten, daß eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung der Benutzerin oder des Benutzers festgestellt worden ist.

(2) Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.

(3) Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der datenverarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die datenverarbeitende Stelle hat sicherzustellen, daß sie die Daten entschlüsseln kann.

(4) Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Die Protokolldatenbestände sind ein Jahr zu speichern. Es ist sicherzustellen, daß die Verfahren und Geräte, mit denen die gespeicherten Daten lesbar gemacht werden können, verfügbar sind.

(5) Die datenverarbeitenden Stellen haben die ordnungsgemäße Anwendung der automatisierten Verfahren zu überwachen.

§ 7
Verfahrensverzeichnis, Meldung

(1) Die datenverarbeitende Stelle erstellt für jedes von ihr betriebene automatisierte Verfahren ein Verfahrensverzeichnis. Dieses Verzeichnis kann auch von einer Stelle für andere geführt werden. Es enthält Angaben über

1. Name und Anschrift der datenverarbeitenden Stelle,
2. Zweckbestimmung und Rechtsgrundlage des Verfahrens,
3. den Kreis der Betroffenen,
4. die Kategorien der verarbeiteten Daten,
5. die Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden,
6. geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union,
7. die datenschutzrechtliche Beurteilung der oder des behördlichen Datenschutzbeauftragten, soweit eine solche vorliegt,
8. eine allgemeine Beschreibung der nach §§ 5 und 6 zur Einhaltung der Datensicherheit getroffenen Maßnahmen.

(2) Absatz 1 gilt nicht für Register, die zur Information der Öffentlichkeit bestimmt sind oder die allen Personen, die mindestens ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offenstehen, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

(3) Die datenverarbeitenden Stellen, die keine behördliche Datenschutzbeauftragte und keinen behördlichen Datenschutzbeauftragten nach § 10 bestellt haben, melden der oder dem Landesbeauftragten für Datenschutz den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens. Ausgenommen sind die in den Absätzen 2 und 4 genannten Verfahren. Die meldepflichtigen Stellen haben spätestens bei der ersten Einspeicherung die Angaben nach Absatz 1 mitzuteilen. Bei Verfahren, die von öffentlichen Stellen entwickelt worden sind, können diese Stellen mit der Abgabe der Meldung beauftragt werden.

(4) Die oder der Landesbeauftragte für Datenschutz führt ein Verzeichnis der Meldungen nach Absatz 3. Es enthält die Angaben nach Absatz 1. Das Verzeichnis kann von jeder Person eingesehen werden. Satz 3 gilt nicht für Verfahren, die

1. nach dem Landesverfassungsschutzgesetz geführt werden,
2. der Gefahrenabwehr dienen,
3. der Strafverfolgung dienen oder
4. der Steuerfahndung dienen,

soweit die datenverarbeitende Stelle eine Einsichtnahme mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

(5) Bei Bestellung einer oder eines behördlichen Datenschutzbeauftragten nach § 10 kann das Verfahrensverzeichnis von jeder Person bei der datenverarbeitenden Stelle eingesehen werden. Die Ausnahmen von der Einsicht nach Absatz 4 Satz 4 gelten entsprechend.

§ 8
Gemeinsame Verfahren und Abrufverfahren

(1) Ein automatisiertes Verfahren, das mehreren datenverarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten (gemeinsames Verfahren) oder die Übermittlung personenbezogener Daten durch Abruf (Abrufverfahren) ermöglicht, darf nur eingerichtet werden, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Verfahrens kontrolliert werden kann. Hierzu ist das Verfahrensverzeichnis nach § 7 Abs. 1 um die Feststellung zu ergänzen, für welchen Bereich der Datenverarbeitung jede der beteiligten Stellen verantwortlich ist. Die Betroffenen können die ihnen nach Abschnitt V dieses Gesetzes zustehenden Rechte gegenüber jeder der beteiligten Stellen geltend machen. Diese leiten die Anliegen der Betroffenen an die nach Satz 2 als verantwortlich festgestellte Stelle weiter.

(3) Werden bei gemeinsamen Verfahren personenbezogene Daten übermittelt, so sind die Empfänger, der Zeitpunkt der Übermittlung und die jeweils übermittelten Daten zu protokollieren. Die Protokolldatenbestände sind ein Jahr zu speichern.

(4) Bei Abrufverfahren trägt die Verantwortung für die Zulässigkeit des einzelnen Abrufs die abrufende Stelle. Die speichernde Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlaß besteht. Die speichernde Stelle hat zu gewährleisten, daß die Zulässigkeit der Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offenstehen oder deren Veröffentlichung zulässig wäre.

§ 9
Vorabkontrolle

(1) Vor der Einrichtung oder wesentlichen Änderung
1. eines Verfahrens nach § 8 Abs. 1 oder
2. eines automatisierten Verfahrens, in dem Daten im Sinne des § 11 Abs. 3 verarbeitet werden,

ist der oder dem behördlichen Datenschutzbeauftragten oder, wenn eine solche oder ein solcher nicht bestellt ist, der oder dem Landesbeauftragten für Datenschutz Gelegenheit zur Prüfung innerhalb einer angemessenen Frist zu geben, ob die Datenverarbeitung zulässig und die vorgesehenen Maßnahmen nach §§ 5 und 6 ausreichend sind (Vorabkontrolle).

(2) Absatz 1 gilt nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offenstehen oder deren Veröffentlichung zulässig wäre.

§ 10
Behördliche Datenschutzbeauftragte

(1) Die datenverarbeitende Stelle kann schriftlich eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen. Mehrere datenverarbeitende Stellen können gemeinsam eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen.

(2) Die oder der behördliche Datenschutzbeauftragte muß die erforderliche Sachkunde und Zuverlässigkeit besitzen. Sie oder er darf durch die Bestellung keinem Konflikt mit anderen dienstlichen Aufgaben ausgesetzt sein.

(3) Die oder der behördliche Datenschutzbeauftragte ist unmittelbar der Leiterin oder dem Leiter der datenverarbeitenden Stelle zu unterstellen. Sie oder er ist bei der Ausübung des Amtes weisungsfrei und darf wegen der Wahrnehmung des Amtes nicht benachteiligt werden. Sie oder er ist zur Erfüllung der Aufgaben des Amtes im erforderlichen Umfang freizustellen und mit den notwendigen Mitteln auszustatten. Beschäftigte und Betroffene können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an sie oder ihn wenden. Die oder der behördliche Datenschutzbeauftragte darf zur Aufgabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen. Dies gilt nicht, soweit besondere Amts- und Berufsgeheimnisse dem entgegenstehen. Im übrigen gilt § 35 Abs. 1 entsprechend.

(4) Die oder der behördliche Datenschutzbeauftragte überwacht und unterstützt die Einhaltung der datenschutzrechtlichen Vorschriften bei der datenverarbeitenden Stelle. Sie oder er hat insbesondere

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken,
2. die Beschäftigten der datenverarbeitenden Stellen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die datenverarbeitende Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten zu beraten und bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren auf die Einhaltung der einschlägigen Vorschriften hinzuwirken,
4. das Verzeichnis nach § 7 Abs. 1 zu führen und zur Einsicht bereitzuhalten,
5. die Vorabkontrolle nach § 9 Abs. 1 durchzuführen.

In Zweifelsfällen hat sie oder er die Landesbeauftragte oder den Landesbeauftragten für Datenschutz zu hören.

Abschnitt II
Zulässigkeit der Datenverarbeitung

§ 11
Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. die oder der Betroffene eingewilligt hat,
2. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt,
3. sie zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der datenverarbeitenden Stelle erforderlich ist oder
4. sie zur Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist.

(2) Die Verarbeitung personenbezogener Daten, die allgemein zugänglichen Quellen entnommen werden können, sowie von Daten, die die Betroffenen selbst zur Veröffentlichung bestimmt haben, ist über die Fälle von Absatz 1 hinaus zulässig, soweit schutzwürdige Belange der Betroffenen nicht beeinträchtigt sind.

(3) Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben sowie von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, ist nur zulässig, soweit

1. die oder der Betroffene eingewilligt hat,
2. die Voraussetzungen des § 17 Abs. 5 oder der §§ 22 bis 25 vorliegen,
3. andere Rechtsvorschriften sie erlauben,
4. sie ausschließlich im Interesse der oder des Betroffenen liegt,
5. sie sich auf Daten bezieht, die die oder der Betroffene selbst öffentlich gemacht hat,

6. sie zur Geltendmachung rechtlicher Ansprüche vor Gericht erforderlich ist oder
7. sie für die Abwehr von Gefahren für Leben, Gesundheit, persönliche Freiheit oder vergleichbare Rechtsgüter erforderlich ist.

Satz 1 gilt entsprechend für Daten über strafbare Handlungen und Entscheidungen in Strafsachen.

(4) Die Datenverarbeitung soll so organisiert sein, daß bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so sind auch die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der oder des Betroffenen überwiegen. Die nicht erforderlichen Daten unterliegen insoweit einem Verwertungsverbot.

(5) Die Absätze 3 und 4 finden keine Anwendung, wenn die Datenverarbeitung

1. durch die Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben erfolgt,
2. der Gefahrenabwehr dient,
3. der Strafverfolgung dient oder
4. der Steuerfahndung dient.

Absatz 3 Satz 1 findet keine Anwendung, wenn die Datenverarbeitung der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder der Verwaltung von Gesundheitsdiensten dient und die Verarbeitung der Daten durch ärztliches Personal oder sonstige Personen, die einer der ärztlichen Schweigepflicht entsprechenden Geheimhaltungspflicht unterliegen, erfolgt.

(6) Pseudonymisierte Daten dürfen nur von solchen Stellen verarbeitet werden, die keinen Zugriff auf die Zuordnungsfunktion haben. Die Übermittlung pseudonymisierter Daten ist zulässig, wenn die Zuordnungsfunktion im alleinigen Zugriff der übermittelnden Stelle verbleibt.

§ 12
Form der Einwilligung

(1) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. In den Fällen des § 11 Abs. 3 muß sich die Einwilligung ausdrücklich auf die dort aufgeführten Daten beziehen. Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, ist die oder der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen.

(2) Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

(3) Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, daß

1. sie nur durch eine eindeutige und bewußte Handlung der oder des Betroffenen erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihre Urheberin oder ihr Urheber erkannt werden kann und
4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird.

§ 13
Erhebung, Zweckbindung

(1) Personenbezogene Daten sind bei den Betroffenen mit ihrer Kenntnis zu erheben. Ohne Kenntnis der Betroffenen dürfen personenbezogene Daten nur erhoben werden, wenn die Voraussetzungen von Absatz 3 Nr. 1, 2 oder 4 vorliegen. Die Herkunft der Daten ist zu dokumentieren.

(2) Personenbezogene Daten dürfen nur für den Zweck weiterverarbeitet werden, für den sie rechtmäßig erhoben worden sind. Daten, von denen die öffentliche Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für die Zwecke weiterverarbeitet werden, für die sie erstmals rechtmäßig gespeichert worden sind.

(3) Die Verarbeitung für andere Zwecke ist ohne Einwilligung der oder des Betroffenen nur zulässig, wenn

1. eine Rechtsvorschrift dies erlaubt,
2. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte einzelner dies gebietet,
3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder
4. die Einholung der Einwilligung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre und offensichtlich ist, daß die Verarbeitung im Interesse der oder des Betroffenen liegt und sie oder er in Kenntnis des anderen Zwecks die Einwilligung erteilen würde.

(4) Daten im Sinne von § 11 Abs. 3 Satz 1 dürfen ohne Einwilligung der oder des Betroffenen für andere Zwecke nur verarbeitet werden, wenn die Voraussetzungen des Absatzes 3 Nr. 1 oder 2 vorliegen. Dies gilt nicht in den Fällen des § 11 Abs. 5.

(5) Die Verarbeitung der Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zur Rechnungsprüfung gilt nicht als Verarbeitung für andere Zwecke. Die Verarbeitung zu Ausbildungs- und Prüfungszwecken hat in anonymisierter oder pseudonymisierter Form zu erfolgen. Lassen sich die in Satz 2 genannten Zwecke durch anonymisierte oder pseudonymisierte Datenverarbeitung nicht erreichen, so ist die Zweckänderung zulässig, soweit berechtigte Interessen der oder des Betroffenen an der Geheimhaltung der Daten nicht überwiegen.

(6) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

(7) Werden Daten innerhalb einer datenverarbeitenden Stelle zu einem anderen Zweck als dem nach Absatz 2 weiterverarbeitet, so ist dies zu dokumentieren.

§ 14
Datenübermittlung an andere öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, wenn die Voraussetzungen der §§ 11 und 13 Abs. 2 bis 6 vorliegen.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Soll die Übermittlung auf Ersuchen einer Stelle erfolgen, so hat diese die hierfür erforderlichen Angaben zu machen, insbesondere die Rechtsgrundlage für die Übermittlung anzugeben. Die übermittelnde Stelle prüft die Schlüssigkeit der Anfrage. Bestehen im Einzelfall Zweifel, so prüft sie auch die Rechtmäßigkeit des Ersuchens.

§ 15
Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. von diesen ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt sind oder
2. die Voraussetzungen der §§ 11 und 13 vorliegen.

(2) Die übermittelnde Stelle hat die empfangende Stelle zu verpflichten, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihr übermittelt wurden.

§ 16
Datenübermittlung an ausländische Stellen

(1) Die Zulässigkeit der Übermittlung an öffentliche und nicht-öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes richtet sich nach §§ 14 und 15.

(2) Die Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union ist nur zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Fehlt es an einem angemessenen Datenschutzniveau, so ist die Übermittlung nur zulässig, wenn

1. die oder der Betroffene eingewilligt hat,
2. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung eines rechtlichen Interesses erforderlich ist,
3. die Übermittlung zur Wahrung lebenswichtiger Interessen der oder des Betroffenen erforderlich ist,
4. die Übermittlung aus einem für die Öffentlichkeit bestimmten Register erfolgt oder
5. die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes der Grundrechte bietet.

(3) Vor der Entscheidung über die Angemessenheit des Datenschutzniveaus und einer Entscheidung nach Absatz 2 Nr. 5 ist die oder der Landesbeauftragte für Datenschutz zu hören.

(4) Die empfangende Stelle ist darauf hinzuweisen, daß die Daten nur zu den Zwecken verarbeitet werden dürfen, für die sie übermittelt wurden.

Abschnitt III
Besondere Formen der Datenverarbeitung

§ 17
Verarbeitung personenbezogener Daten im Auftrag, Wartung

(1) Läßt eine datenverarbeitende Stelle personenbezogene Daten in ihrem Auftrag verarbeiten, bleibt sie für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Rechte der Betroffenen sind ihr gegenüber geltend zu machen. Die Weitergabe der Daten von der datenverarbeitenden Stelle an die Auftragnehmenden gilt nicht als Übermittlung im Sinne von § 2 Abs. 2 Nr. 3.

(2) Die datenverarbeitende Stelle hat dafür Sorge zu tragen, daß personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. Sie hat Auftragnehmende unter besonderer Berücksichtigung ihrer Eignung für die Gewährleistung der nach den §§ 5 und 6 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Aufträge, ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und die etwaige Zulässigkeit von Unterauftragsverhältnissen sind schriftlich festzulegen.

(3) Sofern die Vorschriften dieses Gesetzes auf Auftragnehmende keine Anwendung finden, hat die datenverarbeitende Stelle diese zu verpflichten, jederzeit von ihr veranlaßte Kontrollen zu ermöglichen.

(4) Bei der Erbringung von Wartungsarbeiten oder von vergleichbaren Unterstützungstätigkeiten bei der Datenverarbeitung durch Stellen oder Personen außerhalb der datenverarbeitenden Stelle gelten die Absätze 1 bis 3 entsprechend.

(5) Zur Durchführung von beratenden oder begutachtenden Tätigkeiten im Auftrag der datenverarbeitenden Stelle ist die Übermittlung personenbezogener Daten zulässig, wenn die übermittelnde Stelle die beauftragten Personen verpflichtet,

1. die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihnen überlassen worden sind und
2. nach Erledigung des Auftrags die ihnen von der datenverarbeitenden Stelle überlassenen Datenträger zurückzugeben und die bei ihnen gespeicherten Daten zu löschen, soweit nicht besondere Rechtsvorschriften entgegenstehen.

Die Absätze 1 bis 3 gelten entsprechend.

§ 18
Mobile personenbezogene Datenverarbeitungssysteme

(1) Informationstechnische Systeme zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten automatisiert austauschen können (mobile Datenverarbeitungssysteme, z.B. Chipkarten), dürfen nur mit der Einwilligung der oder des Betroffenen oder aufgrund einer Rechtsvorschrift eingesetzt werden.

(2) Für die Betroffenen muß jederzeit erkennbar sein,

1. ob Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlaßt stattfinden,
2. welche personenbezogenen Daten der oder des Betroffenen verarbeitet werden und
3. welcher Verarbeitungsvorgang im einzelnen abläuft oder angestoßen wird.

(3) Die Betroffenen sind bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihnen nach §§ 26 ff. zustehenden Rechte aufzuklären.

§ 19
Automatisierte Einzelentscheidungen

Entscheidungen, die zu einer tatsächlichen oder rechtlichen Beschwer der Betroffenen führen, dürfen nicht ausschließlich auf die Ergebnisse automatisierter Verfahren, die einzelne Aspekte der Person der Betroffenen bewerten, gestützt werden. Ergebnisse automatisierter Verfahren dürfen abweichend von Satz 1 für Entscheidungen verwendet werden, wenn

1. ein Gesetz dies vorsieht oder
2. der oder dem Betroffenen vor der Entscheidung ermöglicht wird, ihre oder seine besonderen persönlichen Interessen geltend zu machen.

§ 20
Video-Überwachung und -Aufzeichnung

(1) Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten (Video-Überwachung), soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Belange Betroffener nicht überwiegen.

(2) Das Bildmaterial darf gespeichert werden (Video-Aufzeichnung), wenn die Tatsache der Aufzeichnung für die Betroffenen durch geeignete Maßnahmen erkennbar gemacht ist. Die Aufzeichnungen sind spätestens nach sieben Tagen zu löschen, es sei denn, sie dokumentieren Vorkommnisse, zu deren Aufklärung die weitere Speicherung erforderlich ist.

§ 21
Fernmessen und Fernwirken

(1) Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen, insbesondere in der Wohnung oder in den Geschäftsräumen ferngesteuert Messungen vorzunehmen oder andere Wirkungen auszulösen, bedarf dessen Einwilligung.

(2) Eine Leistung, der Abschluß oder die Abwicklung eines Vertragsverhältnisses darf nicht von der Einwilligung der oder des Betroffenen nach Absatz 1 abhängig gemacht werden. Verweigert oder widerruft die oder der Betroffene ihre oder seine Einwilligung, so dürfen ihr oder ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

Abschnitt IV
Besondere Zwecke der Datenverarbeitung

§ 22
Datenverarbeitung für wissenschaftliche Zwecke

(1) Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken durch öffentliche Stellen und die Übermittlung personenbezogener Daten durch öffentliche Stellen an Dritte, die die Daten zu wissenschaftlichen Zwecken nutzen wollen (Datenverarbeitung für wissenschaftliche Zwecke), soll in anonymisierter Form erfolgen. Ist eine Anonymisierung nicht möglich, sollen die Daten pseudonymisiert werden. § 11 Abs. 6 gilt entsprechend.

(2) Steht bei der übermittelnden Stelle zur Erfassung der Daten, zur Anonymisierung oder Pseudonymisierung nicht ausreichend Personal zur Verfügung, so können die mit der Forschung befaßten Personen diese Aufgaben wahrnehmen, wenn sie zuvor zur Verschwiegenheit verpflichtet worden sind.

(3) Ist weder eine Anonymisierung noch eine Pseudonymisierung möglich, ist die Datenverarbeitung für wissenschaftliche Zwecke zulässig, wenn

1. die oder der Betroffene in die Datenverarbeitung eingewilligt hat,
2. es sich nicht um Daten nach § 11 Abs. 3 handelt und schutzwürdige Belange der oder des Betroffenen wegen der Art der Daten oder wegen der Art der Verwendung für das jeweilige Forschungsvorhaben nicht beeinträchtigt sind oder
3. die Genehmigung der für die datenverarbeitende Stelle zuständigen obersten Aufsichtsbehörde vorliegt.

(4) Die Genehmigung nach Absatz 3 Nr. 3 wird erteilt, wenn das öffentliche Interesse an der Durchführung des jeweiligen Forschungsvorhabens die schutzwürdigen Belange der oder des Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Die Genehmigung muß den Forschungszweck, die Art der zu verarbeitenden Daten, den Kreis der Betroffenen sowie bei Übermittlungen den Empfängerkreis bezeichnen und ist der oder dem Landesbeauftragten für den Datenschutz mitzuteilen.
(5) Sobald der Forschungszweck es gestattet, sind die Daten zu anonymisieren, hilfsweise zu pseudonymisieren. Nach Maßgabe der Absätze 1 bis 3 dürfen die personenbezogenen Daten auch für einen anderen als den ursprünglichen Forschungszweck weiterverarbeitet werden.

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

1. die oder der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Personen der Zeitgeschichte unerläßlich ist.

(7) Die übermittelnde Stelle hat empfangende Stellen, auf die dieses Gesetz keine Anwendung findet, zu verpflichten, die Vorschriften der Absätze 5 und 6 einzuhalten und jederzeit Kontrollen durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz zu ermöglichen.

§ 23
Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Öffentliche Stellen dürfen Daten der Beschäftigten vorbehaltlich besonderer gesetzlicher oder tarifvertraglicher Regelungen nur nach Maßgabe der §§ 106 bis 106 h des Landesbeamtengesetzes verarbeiten.

(2) Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 gespeichert oder in einem automatisierten Verfahren gewonnen werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

§ 24
Öffentliche Auszeichnungen

(1) Zur Vorbereitung öffentlicher Auszeichnungen dürfen die Ministerpräsidentin oder der Ministerpräsident, das Innenministerium sowie die von der Ministerpräsidentin oder dem Ministerpräsidenten besonders beauftragten Stellen die dazu erforderlichen personenbezogenen Daten auch ohne Kenntnis der Betroffenen erheben und weiterverarbeiten.

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

(3) § 27 findet keine Anwendung.

§ 25
Besondere Dokumentationsstelle für Sekten

(1) Die Ministerpräsidentin oder der Ministerpräsident oder eine von ihr oder von ihm besonders beauftragte Stelle (Dokumentationsstelle) kann zum Zweck der Aufklärung oder Warnung die Betätigungen von Sekten oder sektenähnlichen Vereinigungen einschließlich der mit ihnen rechtlich, wirtschaftlich oder in ihrer religiösen oder weltanschaulichen Zielsetzung verbundenen Organisationen oder Vereinigungen in Schleswig-Holstein dokumentieren und über sie informieren, sofern tatsächliche Anhaltspunkte den Verdacht begründen, daß von deren Wirken Gefahren für die Menschenwürde, die freie Entfaltung der Persönlichkeit, das Leben, die Gesundheit oder das Eigentum ausgehen, insbesondere daß Personen in ihrer Willensfreiheit eingeschränkt werden.

(2) Soweit ein begründeter Verdacht im Sinne des Absatz 1 besteht, kann die Dokumentationsstelle über Personen, die in einer derartigen Sekte, Vereinigung oder Organisation aktiv mitwirken, bei anderen öffentlichen Stellen vorhandene oder öffentlich zugängliche personenbezogene Daten erheben und weiterverarbeiten. Hiervon ausgenommen sind Daten, die besonderen Berufs- oder Amtsgeheimnissen unterliegen, sowie Daten, für die besondere Verwendungsvorschriften in anderen Gesetzen bestehen.

(3) Die Speicherung der erhobenen personenbezogenen Daten ist spätestens nach zwei Jahren auf ihre Erforderlichkeit zu prüfen. Spätestens fünf Jahre nach der letzten Tätigkeit im Sinne von Absatz 2 sind die personenbezogenen Daten zu löschen.

(4) An Stellen außerhalb des öffentlichen Bereichs dürfen personenbezogene Daten übermittelt werden, wenn

1. es zur Erfüllung der Aufgabe nach Absatz 1 erforderlich ist oder
2. ein Dritter ein rechtliches Interesse daran hat

und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt sind.

Abschnitt V
Rechte der Betroffenen

§ 26
Aufklärung, Benachrichtigung

(1) Werden personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis erhoben, so sind sie in geeigneter Weise aufzuklären über

1. die Anschrift der datenverarbeitenden Stelle,
2. den Zweck der Datenerhebung,
3. die Rechtsvorschrift, die die Datenverarbeitung gestattet; liegt eine solche nicht vor, die Freiwilligkeit der *Datenangabe*,
4. die Folgen einer Nichtbeantwortung, wenn die Angaben für die Gewährung einer Leistung erforderlich sind,
5. ihre Rechte nach diesem Gesetz,

6. den Empfängerkreis bei beabsichtigten Übermittlungen sowie
7. die Auftragnehmenden bei beabsichtigter Datenverarbeitung im Auftrag.

(2) Absatz 1 gilt nicht für

1. die Verfassungsschutzbehörden,
2. die Behörden der Staatsanwaltschaft,
3. die Behörden der Polizei,
4. die Gefahrenabwehrbehörden und
5. die Landesfinanzverwaltungen.

(3) Werden die Daten ohne Kenntnis der Betroffenen erhoben, so sind diese in angemessener Weise über die verarbeiteten Daten und über die in Absatz 1 Satz 1 Nr. 1 bis 3 und 5 bis 7 genannten Umstände zu unterrichten. Absatz 1 Satz 2 gilt entsprechend. Sollen die Daten übermittelt werden, so hat die Benachrichtigung spätestens zeitgleich mit der Übermittlung zu erfolgen. Sätze 1 und 2 finden keine Anwendung, wenn die Betroffenen auf andere Weise Kenntnis von der Verarbeitung ihrer Daten erlangt haben.

§ 27
Auskunft an Betroffene

(1) Den Betroffenen ist von der datenverarbeitenden Stelle auf Antrag Auskunft zu erteilen über

1. die zu ihrer Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Speicherung,
3. die Herkunft der Daten und den Empfängerkreis von Übermittlungen,
4. die Auftragnehmenden bei Datenverarbeitung im Auftrag,
5. die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den gesetzlichen Bestimmungen entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind, sowie
6. die Funktionsweise von automatisierten Verfahren.

Die Betroffenen sollen die Art der personenbezogenen Daten, über die Auskunft verlangt wird, näher bezeichnen.

(2) Den Betroffenen kann statt der Auskunft Einsicht in die zu ihrer Person gespeicherten Daten gewährt werden. Die Einsicht wird nicht gewährt, soweit diese mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(3) Die Auskunftserteilung oder die Gewährung von Einsicht unterbleibt, soweit eine Prüfung ergibt, daß

1. dadurch die Erfüllung der Aufgaben der datenverarbeitenden Stelle, einer übermittelnden Stelle oder einer empfangenden Stelle gefährdet würde,

2. dadurch die öffentliche Sicherheit gefährdet würde oder sonst dem Wohle des Bundes oder eines Landes schwere Nachteile entstehen würden oder
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(4) Werden Auskunft oder Einsicht nicht gewährt, ist die oder der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, daß sie oder er sich an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz wenden kann. Eine Begründung für die Auskunftsverweigerung erfolgt nicht, soweit dadurch der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

§ 28
Berichtigung, Löschung, Sperrung

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

(2) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Die datenverarbeitende Stelle legt in allgemeinen Regelungen über die Aufbewahrung von Daten den Zeitraum fest, innerhalb dessen die Daten als zur Aufgabenerfüllung erforderlich gelten. Sind personenbezogene Daten in Akten untrennbar im Sinne von § 11 Abs. 4 Satz 2 gespeichert, ist die Löschung nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist.

(3) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit von der oder dem Betroffenen bestritten wird und sich weder Richtigkeit noch die Unrichtigkeit nachweisen läßt,
2. sie zur Aufgabenerfüllung nicht mehr erforderlich sind, Rechtsvorschriften jedoch die weitere Aufbewahrung anordnen,
3. die oder der Betroffene anstelle der Löschung die Sperrung verlangt,
4. die Löschung die Betroffene oder den Betroffenen in der Verfolgung ihrer oder seiner Rechte oder in sonstigen schutzwürdigen Belangen beeinträchtigen würde oder
5. eine Löschung gemäß Absatz 2 Satz 3 nicht erfolgt.

(4) Gesperrte Daten dürfen über die Speicherung hinaus ohne Einwilligung der oder des Betroffenen nicht mehr weiterverarbeitet werden, es sei denn, daß Rechtsvorschriften die Verarbeitung zulassen oder die Nutzung durch die datenverarbeitende Stelle zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der datenverarbeitenden Stelle oder von Dritten liegenden Gründen unerläßlich ist. Die Gründe für die Nutzung gesperrter Daten sind zu dokumentieren.

(5) Von der Berichtigung, Sperrung oder Löschung nach Absatz 2 Nr. 1 sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt wurden. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt werden.

§ 29
Einwand gegen die Verarbeitung

(1) Die Betroffenen haben das Recht, schriftlich unter Hinweis auf besondere persönliche Gründe Einwand gegen die Verarbeitung ihrer Daten allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben. Der Einwand ist begründet, wenn ein schutzwürdiges Interesse der oder des Betroffenen das öffentliche Interesse an der Datenverarbeitung im Einzelfall überwiegt. In diesem Fall ist die Datenverarbeitung insgesamt oder in bestimmten Formen unzulässig.

(2) Absatz 1 findet keine Anwendung bei Verfahren, die

1. nach dem Landesverfassungsschutzgesetz geführt werden,
2. der Gefahrenabwehr dienen,
3. der Strafverfolgung dienen oder
4. der Steuerfahndung dienen.

§ 30
Schadensersatz

(1) Entsteht der oder dem Betroffenen durch eine unzulässige oder unrichtige Verarbeitung ihrer oder seiner personenbezogenen Daten in einem automatisierten Verfahren ein Schaden, so ist ihr oder ihm der Träger jeder für die Verarbeitung verantwortlichen Stelle unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) In Fällen einer schweren Verletzung des Persönlichkeitsrechts kann die oder der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen.

(3) Die ersatzpflichtige Stelle haftet jeder oder jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 125.000 Euro. Mehrere Ersatzpflichtige haften gesamtschuldnerisch.

(4) Auf das Mitverschulden der oder des Betroffenen und die Verjährung des Entschädigungsanspruchs sind §§ 254, 839 Abs. 3 und § 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(5) Die Geltendmachung weitergehender Schadensersatzansprüche aufgrund anderer Vorschriften bleibt unberührt.

§ 31
Unabdingbarkeit

Die Rechte der Betroffenen aus diesem Gesetz können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

Abschnitt VI
Die oder der Landesbeauftragte für Datenschutz
(Regelung überwiegend durch „vorgeschaltetes" Änderungsgesetz zum geltenden LDSG)

§ 32
Berufung und Rechtsstellung
(Regelung durch „vorgeschaltetes" Änderungsgesetz zum geltenden LDSG: Ausgestaltung von der Entscheidung abhängig, ob LD als oberste Landesbehörde oder als Anstalt des öffentlichen Rechts eingerichtet werden soll))

§ 33
Aufgaben der oder des Landesbeauftragten für Datenschutz
(zumindest teilweise Regelung durch „vorgeschaltetes" Änderungsgesetz zum geltenden LDSG)

(1) Die oder der Landesbeauftragte für Datenschutz überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen nach § 3. Sie oder er berät die obersten Landesbehörden sowie die sonstigen öffentlichen Stellen in Fragen des Datenschutzes und der damit zusammenhängenden Datenverarbeitungstechniken sowie der Sozialverträglichkeit. Zu diesem Zweck können Empfehlungen zur Verbesserung des Datenschutzes gegeben werden. Die Gerichte und der Landesrechnungshof unterliegen ihrer oder seiner Kontrolle, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

(2) Die oder der Landesbeauftragte für Datenschutz nimmt die Aufgaben der zuständigen Aufsichtsbehörde nach § 38 Bundesdatenschutzgesetz über nicht-öffentliche Stellen im Anwendungsbereich des Dritten Abschnitts des Bundesdatenschutzgesetzes wahr. Insoweit unterliegt sie oder er der Rechtsaufsicht des Innenministeriums.

(3) Auf Anforderung des Landtages, des Eingabenausschusses des Landtages oder einer obersten Landesbehörde soll die oder der Landesbeauftragte für Datenschutz ferner Hinweisen auf Angelegenheiten und Vorgänge, die ihren oder seinen Aufgabenbereich unmittelbar betreffen, nachgehen.

§ 34
Anrufung der oder des Landesbeauftragten für Datenschutz

Jede oder jeder hat das Recht, sich unmittelbar an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz zu wenden, wenn sie oder er annimmt, daß bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen datenschutzrechtliche Vorschriften verletzt wurden. Dies gilt auch für Beschäftigte der öffentlichen Stellen, ohne daß der Dienstweg einzuhalten ist.

§ 35
Kontrollaufgaben

(1) Die öffentlichen Stellen sind verpflichtet, die oder den Landesbeauftragten für Datenschutz bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihr oder ihm ist dabei insbesondere

1. Auskunft zu erteilen sowie Einsicht in Unterlagen und Dateien zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, besondere Amts- und Berufsgeheimnisse stehen dem nicht entgegen;
2. Zutritt zu Diensträumen zu gewähren.

Die oder der Landesbeauftragte für Datenschutz darf im Rahmen von Kontrollen personenbezogene Daten auch ohne Kenntnis der Betroffenen erheben. Die Benachrichtigung der Betroffenen richtet sich nach § 36 Abs. 4.

(2) Stellt die jeweils zuständige oberste Landesbehörde im Einzelfall fest, daß durch eine mit der Einsicht verbundene Bekanntgabe personenbezogener Daten die Sicherheit des Bundes oder eines Landes gefährdet wird, dürfen die Rechte nach Absatz 1 nur von der oder dem Landesbeauftragten für Datenschutz persönlich oder den von ihr oder ihm schriftlich besonders damit betrauten Beauftragten ausgeübt werden.

§ 36
Beanstandungen

(1) Stellt die oder der Landesbeauftragte für Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten bei öffentlichen Stellen fest, so fordert sie oder er diese zur Mängelbeseitigung auf.

(2) Bei erheblichen Verstößen oder sonstigen erheblichen Mängeln spricht die oder der Landesbeauftragte für Datenschutz gegenüber der öffentlichen Stelle eine Beanstandung aus. Sie oder er kann zuvor die öffentliche Stelle zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auffordern und die zuständige Aufsichtsbehörde über die Beanstandung unterrichten.

(3) Mit der Feststellung von Mängeln und der Beanstandung sollen Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbunden werden.

(4) Die Betroffenen können mit Kenntnis der datenverarbeitenden Stelle nach pflichtgemäßem Ermessen von Verstößen gegen die Vorschriften dieses Gesetzes oder andere Datenschutzvorschriften unterrichtet werden.

§ 37
Serviceaufgaben

(1) Die oder der Landesbeauftragte für Datenschutz berät die öffentlichen Stellen in Fragen des Datenschutzes, der Datensicherheit und der damit zusammenhängenden Datenverarbeitungstechniken sowie deren Sozialverträglichkeit. Zu diesem Zweck können Empfehlungen zur Verbesserung des Datenschutzes gegeben werden. Auf Anforderung des Landtages, einzelner Fraktionen des Landtages oder der Landesregierung hat die oder der Landesbeauftragte für den Datenschutz Gutachten zu erstellen und Berichte zu erstatten.

(2) Die oder der Landesbeauftragte für Datenschutz berät und informiert die Bürgerinnen und Bürger über alle Fragen des Datenschutzes und der Datensicherheit, insbesondere über die ihnen bei der Verarbeitung ihrer Daten zustehenden Rechte sowie über geeignete technische Maßnahmen zum Selbstdatenschutz.

(3) Öffentliche Stellen können ihr Datenschutzkonzept durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz prüfen und beurteilen lassen.

(4) Die oder der Landesbeauftragte für Datenschutz führt Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durch. Sie oder er berät nichtöffentliche Stellen auf Anfrage in Fragen von Datenschutz und Datensicherheit.

(5) Die oder der Landesbeauftragte für Datenschutz kann für die Wahrnehmung der Aufgaben nach den Absätzen 2, 3 und 4 Entgelte erheben.

Abschnitt VII
Schlußvorschriften

§ 38
Ordnungswidrigkeiten

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

1. erhebt, speichert, zweckwidrig verarbeitet, verändert, übermittelt, zum Abruf bereithält oder löscht,
2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung an sich oder andere veranlaßt.

Ordnungswidrig handelt auch, wer anonymisierte oder pseudonymisierte Daten mit anderen Informationen zusammenführt und dadurch die Betroffene oder den Betroffenen wieder bestimmbar macht oder wer sich bei pseudonymisierten Daten entgegen den Vorschriften dieses Gesetzes Zugriff auf die Zuordnungsfunktion verschafft.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

§ 39
Übergangsvorschrift/Inkrafttreten

(1) Soweit in diesem Gesetz Beträge in Euro genannt werden, gelten diese bis zum 31. Dezember 2001 auch als Beträge in DM; der Umrechnungskurs beträgt 1 Euro = 1,95583 DM.

(2) Dieses Gesetz tritt am dritten Tag nach seiner Verkündung in Kraft. Gleichzeitig tritt das Landesdatenschutzgesetz vom 30. Oktober 1991 (GVOBl. Schl.-H. S. 555), zuletzt geändert durch Gesetz vom 12. März 1996 (GVOBl. Schl.-H. S. 291), Zuständigkeiten und Ressortbezeichnungen ersetzt durch Verordnung vom 24. Oktober 1996 (GVOBl. Schl.-H. S. 652), außer Kraft.

Das vorstehende Gesetz wird hiermit ausgefertigt und ist zu verkünden.

Kiel,

Heide Simonis
Ministerpräsidentin

Dr. Ekkehard Wienholtz
Innenminister

Begründung

A. Allgemeines:

Anlaß für die Neufassung des Schleswig-Holsteinischen Datenschutzgesetzes ist die Richtlinie des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, die nach Art. 32 Abs. 1 in nationales Recht umzusetzen ist.

Die Richtlinie gilt vorrangig für die in die Gesetzgebungszuständigkeit des Bundes fallende Privatwirtschaft, aber auch für den größtenteils in den Landesgesetzen geregelten Datenschutz in der öffentlichen Verwaltung.

Über die Anpassung an die Richtlinie hinaus wird die Novellierung des Landesdatenschutzgesetzes zum Anlaß genommen,

- auf Veränderungen der Technik datenschutzrechtlich zu reagieren (Regelung zu mobilen Datenverarbeitungssystemen wie z.B. Chipkarten36,

- die Prinzipien der Datenvermeidung und Datensparsamkeit sowie der frühestmöglichen Anonymisierung und Pseudonymisierung stärker zu betonen,

- das Erfordernis eines Datenschutzes durch Technik zu normieren,

- ein Datenschutz-Audit einzuführen und

- die Serviceorientierung des Datenschutzes auszubauen.

Soweit möglich, werden die datenschutzrechtlichen Vorschriften und Verfahren vereinfacht und „entbürokratisiert".

B. Einzelbegründung:

Zu § 1

Der Schutzzweck des Gesetzes ist unverändert geblieben. Da das Recht auf informationelle Selbstbestimmung als eine Komponente des in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verankerten Grundrechts auf freie Entfaltung der Persönlichkeit in der Rechtspraxis hinlänglich konkretisiert ist, kann auf eine gesetzliche Definition des Begriffs verzichtet werden.

Zu § 2

Die Bestimmungen der Absätze 1 bis 3 sind im wesentlichen unverändert geblieben. Insgesamt wurden die Formulierungen aber gestrafft. *Der bisherige Absatz 4 wurde inhaltlich in Absatz 5 übernommen. Die bisherigen Absätze 5 und 6 wurden ersatzlos gestrichen, da die dort definierten Begriffe aus sich selbst heraus verständlich bzw. in der Rechtspraxis hinlänglich konkretisiert sind.*

Absatz 2

Gegenüber der früheren Formulierung wird nun stärker verdeutlicht, daß „Datenverarbeitung" als Verwendung personenbezogener Daten ein umfassender Oberbegriff ist.

Auf die Definition der sich aus sich selbst erklärenden Begriffe „"Verändern" und „Nutzen" wurde verzichtet. Neu aufgenommen und erläutert wurden als Nummern 7 und 8 dagegen die Begriffe „Pseudonymisieren" und „Verschlüsseln". Auch diese Vorgänge fallen unter den Oberbegriff der Datenverarbeitung.

Die Wirkung des Pseudonymisierens kommt der des Anonymisierens nahe; ein Unterschied besteht jedoch darin, daß sich bei Verwendung derselben Zuordnungsfunktion Informationen aus unterschiedlichen Kontexten über eine Person zusammenführen lassen. Ebenso wie beim Anonymisieren geht die Definition von der Frage aus, ob bestimmte Informationen den Betroffenen zugeordnet werden können. Im Unterschied zum Anonymisieren besteht beim Pseudonymisieren aber eine Zuordnungsfunktion, ohne die eine Zuordnung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Die Aufnahme einer Definition des „Verschlüsselns" trägt der zunehmenden Bedeutung dieses Vorgangs Rechnung.

Absätze 4 und 5

Da das Gesetz entsprechend der Terminologie der EG-Datenschutzrichtlinie an verschiedenen Stellen zwischen „Empfängern" von Daten und „Dritten" unterscheidet, wurden hier zur Klarstellung die Legaldefinitionen des Art. 2 Buchst. f und g der EG-Datenschutzrichtlinie in angepaßter Form übernommen.

Zu § 3

Absatz 1

Der Regelungsgehalt der Nummer 1 entspricht dem bisherigen Absatz 1. Mit der neuen Regelung der Nummer 2 wird - wie schon in den Datenschutzgesetzen einiger anderer Länder - die in § 2 Absätze 2 und 3 BDSG eröffnete Regelungsbefugnis für die Länder ausgeschöpft. Die Gleichbehandlung dieser Stellen mit öffentlichen Stellen ist sachgerecht, soweit öffentliche Aufgaben in privatrechtlicher Form wahrgenommen werden. Dadurch wird vermieden, daß allein die Wahl der Rechtsform bereits Auswirkung auf die Rechtsstellung der Betroffenen hat.

Absatz 2

Die bisherigen Absätze 2 und 3 sind zusammengefaßt und inhaltlich an den neu gefaßten Absatz 1 angepaßt worden.

Der frühere Absatz 4 ist nicht wiederaufgenommen worden. Zwar sind öffentliche Stellen in Begnadigungsverfahren nur einer geringen rechtlichen Bindung unterworfen, jedoch besteht im Hinblick auf das informationelle Selbstbestimmungsrecht kein Anlaß, diesen Bereich auch von der Geltung des LDSG auszunehmen.

Da der Datenschutz bei den Rundfunkanstalten bereichsspezifisch durch die Rundfunkstaatsverträge geregelt ist, kann auf den bisherigen Absatz 5 ersatzlos verzichtet werden.

Absatz 3

Dieser Absatz entspricht dem bisherigen Absatz 6 und stellt wie bisher den Vorrang bereichsspezifischer Vorschriften vor dem LDSG klar.

Zu § 4

Absatz 1

Die Regelung stellt den Grundsatz der Datenvermeidung und -sparsamkeit bei der Gestaltung und Beschaffung von automatisierten und nichtautomatisierten Datenverarbeitungsverfahren auf. Dieser ist vom Grundsatz der Erforderlichkeit abzugrenzen: Während die Erforderlichkeit als rechtliche Anforderung den Umfang der Datenverarbeitung in jedem Einzelfall beschränkt, beschreibt der Grundsatz der Datenvermeidung und -sparsamkeit vor allem Gestaltungsanforderungen an IT-Systeme. Beide Kriterien müssen gleichermaßen erfüllt sein. Besondere Bedeutung kommt dem Grundsatz der Datenvermeidung und -sparsamkeit bei der Gestaltung von Verfahren und bei der Auswahl von Produkten zu.

Absatz 2

Es wird die Verpflichtung postuliert, solche Produkte vorrangig zu berücksichtigen, deren Vereinbarkeit mit den rechtlichen Vorgaben (zu denen auch die Datensparsamkeit gehört) in Audits festgestellt wurde. Produkte, die ein solches Verfahren erfolgreich durchlaufen haben, sollen vorrangig eingesetzt werden. Auf diesem Wege sollen die Hersteller angehalten werden, eine freiwillige datenschutzrechtliche Evaluierung ihrer Produkte durchführen zu lassen.

Zu § 5

Die bisher in § 7 enthaltenen sogenannten Zehn Gebote der Datenverarbeitung orientierten sich noch an der Großrechnertechnologie. Die Neuregelung stellt nun die Grundregeln auf, die sowohl bei nichtautomatisierter als auch bei automatisierter Datenverarbeitung einzuhalten sind. Der Katalog der zu treffenden technisch-organisatorischen Maßnahmen ist nicht abschließend.

Absatz 1

Exemplarisch werden drei Sicherheitskomponenten genannt: Die Absicherung der Datenträger gegen unbefugten Zugang, die Schaffung eines definierten Systems von Zugriffsberechtigungen für die Nutzerinnen und Nutzer und die Sicherstellung, daß einzelne Vorgänge der Datenverarbeitung im nachhinein überprüfbar sind. Für nichtautomatisierte Verfahren wird damit im Ergebnis nicht mehr gefordert, als ohnehin von der Rechtsprechung für ordnungsgemäße Aktenführung in der Verwaltung verlangt wird. Dadurch wird gewährleistet, daß trotz der zunehmenden Automatisierung der Verwaltungsabläufe bis hin zum Einsatz von Workflow-Konzepten die Revisionsfähigkeit des Verwaltungshandelns und damit die Rechte der Bürgerinnen und Bürger im Verwaltungsverfahren gewahrt werden.

Absatz 2

Welche Maßnahmen zur Datensicherheit erforderlich sind, ergibt sich im Einzelfall aus einer Abwägung zwischen der Sensibilität und Bedeutung der Daten, dem Grad der Schutzbedürftigkeit und den mit Sicherheitsmaßnahmen verbundenen Kosten. Die Vorschrift fordert außerdem, die technisch-organisatorischen Maßnahmen laufend an den Stand der Technik anzupassen. Um zu gewährleisten, daß automatisierte Verfahren die an sie zu stellenden Anforderungen erfüllen, sind sie vor ihrem Einsatz ausdrücklich freizugeben.

Absatz 3

Die Anforderungen an das Sicherheitskonzept, die Freigabe automatisierter Verfahren und eine ordnungsgemäße Datenverarbeitung sollen im Rahmen einer Verordnung konkretisiert werden.

Zu § 6

Die Vorschrift enthält spezielle Anforderungen an die Gestaltung von automatisierten Verfahren.

Absatz 1

Es wird verlangt, daß mit der Datenverarbeitung erst begonnen werden kann, nachdem die Benutzerinnen und Benutzer ihre Berechtigung im Einzelfall nachgewiesen haben. Dies geschieht regelmäßig durch die Eingabe und Überprüfung von Login und Paßwort. Daneben sind aber auch andere Verfahren denkbar wie z.B. chipkartenbasierte oder biometrische Identifikationsverfahren.

Absatz 2

Die Vorschrift behandelt die notwendigerweise sehr weitreichenden Zugriffsrechte der Systemadministratoren. Zum einen muß der Kreis der Personen, die diese Rechte innehaben, klar definiert sein. Anderen Personen müssen derartige Zugriffe auf die Systemebene technisch unmöglich gemacht werden. Um die „Superuser" nicht ohne Kontrolle zu belassen, müssen die verändernden Zugriffe protokolliert werden. Die Protokolle sind in angemessenen Zeitabständen von der Dienststellenleitung zu kontrollieren.

Absatz 3

Adressat der Vorschrift ist entsprechend der Legaldefinition des § 2 Abs. 3 ausschließlich die datenverarbeitende Stelle selbst. Hierzu zählen nicht die Personen oder Stellen, die im Auftrag für die datenverarbeitende Stelle tätig werden (sie sind „andere" im Sinne des § 2 Abs. 3). Sie unterfallen als öffentliche Stellen (z.B. die Datenzentrale) unmittelbar selbst dem LDSG und als nicht-öffentliche Stellen (z.B. Gewerbetreibende, privatrechtlich organisierte Unternehmen) den Vorschriften des BDSG.

Wird den Beschäftigten die Nutzung von (eigenen oder von der datenverarbeitenden Stelle zur Verfügung gestellten) Computern außerhalb der Räumlichkeiten der datenverarbeitenden Stelle (insbesondere zu Hause) ermöglicht, sind die auf diesen Geräten gespeicherten personenbezogenen Datenbestände zu verschlüsseln. Dies ist für tragbare Computer bisher schon in der Datenschutzverordnung geregelt. Allerdings darf es nicht dazu kommen, daß die datenverarbeitende Stelle keine Möglichkeit mehr hat, an den Informationsgehalt der Daten zu gelangen, falls die Person, die die Verschlüsselung vorgenommen hat, kurzfristig nicht verfügbar ist. Dies läßt sich z.B. dadurch realisieren, daß der datenverarbeitenden Stelle die Verschlüsselungsmethode und der verwendete Schlüssel bekannt sind.

Absatz 4

Die Vorschrift orientiert sich am § 10 Abs. 2 LDSG alter Fassung. In zunehmendem Maße wird auf die Aufbewahrung von papierenen Unterlagen verzichtet und Daten werden ausschließlich in automatisierter Form gespeichert. Auch in diesen Fällen müssen die gleichen Anforderungen an die Nachvollziehbarkeit der Verarbeitung gestellt werden, die für die Datenverarbeitung in Akten gelten. Zu diesem Zweck ist die Speicherung, Veränderung und Übermittlung der Daten zu protokollieren. Außerdem muß sichergestellt werden, daß während der gesamten Speicherungsdauer der Daten die Verfahren und Geräte verfügbar sind, die benötigt werden, um die abgelegten Informationen wieder lesbar machen zu können.

Absatz 5

Die Regelung hat nur deklaratorische Bedeutung, da sich bereits aus dem allgemeinen Verwaltungsrecht die Verpflichtung der datenverarbeitenden Stellen ergibt, für die Einhaltung rechtmäßiger Zustände zu sorgen. Gleichwohl wurden die Vorschriften so wie bisher in das Gesetz aufgenommen, weil durch die spezifischen Schnittstellenprobleme zwischen den Fach- und Technikbereichen in der Verwaltung die Verantwortungsbereiche verwischen.

Der bisherige § 6 S. 1 LDSG (Datengeheimnis) ist verzichtbar. Die im öffentlichen Dienst für das Personal allgemein geltenden Verschwiegenheitspflichten führten schon in der Vergangenheit dazu, daß die Vorschrift weitgehend leerlief. Fehlt es bei einzelnen Stellen an solchen Verschwiegenheitspflichten für das Personal, so kommt § 10 zum Tragen, wonach die Datenverarbeitung nur unter bestimmten Voraussetzungen erlaubt ist. Zwar ist damit zunächst nur den datenverarbeitenden Stellen verboten, Daten darüber hinausgehend zu verarbeiten. Diese Pflicht wird aber durch das zwischen der datenverarbeitenden Stelle und den bei ihr konkret mit der Datenverarbeitung beschäftigten Personen bestehende Rechtsverhältnis umgesetzt und stellt aufgrund dieses Rechtsverhältnisses eine eigene Pflicht der Beschäftigten dar.

Zu § 7

Die Vorschrift setzt Art. 18 der EG-Datenschutzrichtlinie um. Danach ist zur Herstellung von Transparenz und zur besseren Überwachbarkeit der Datenverarbeitung grundsätzlich ein Verfahren vorgesehen, bei dem - ähnlich wie nach § 8 Abs. 1 LDSG a.F. - alle automatisierten Datenverarbeitungen bei der zuständigen Kontrollstelle zu melden sind. In bestimmten Fällen sind Ausnahmen zulässig.

Absatz 1

Nach Art. 18 Abs. 1 der EG-Datenschutzrichtlinie haben die datenverarbeitenden Stellen der jeweiligen Kontrollstelle zu melden, welche automatisierten Verfahren bei ihnen stattfinden. Die bei der Meldung im einzelnen erforderlichen Angaben schreibt Art. 19 Abs. 1 der EG-Datenschutzrichtlinie vor. Dieser Katalog wurde ohne wesentliche Änderung in Abs. 1 übernommen.

Absatz 2

Für bestimmte, einem größeren Personenkreis zugängliche Register gilt Absatz 1 nicht.

Absatz 3

Die Vorschrift setzt Art. 18 Abs. 1 und Art. 19 Abs. 2 der EG-Datenschutzrichtlinie um. Danach haben die öffentlichen Stellen des Landes in dem hier beschriebenen Fall der oder dem Landesbeauftragten für Datenschutz vor Einsatz der automatisierten Verfahren die Meldung mit dem in Abs. 1 beschriebenen Inhalt zu machen.

Absatz 4

Um die Transparenz der Datenverarbeitung zu erhöhen, schreibt Art. 21 Abs. 1 und 2 der EG-Datenschutzrichtlinie vor, daß die Kontrollstellen Verzeichnisse mit den Verfahrensmeldungen zu führen und für jedermann zur Einsicht bereitzuhalten haben. Vom Einsichtsrecht ausgenommen sind die unter Umständen sicherheitskritischen Informationen zur Datensicherheit. Diese Vorgaben setzt Abs. 3 um.

Absatz 5

Wird bei den datenverarbeitenden Stellen eine behördliche Datenschutzbeauftragte oder ein behördlicher Datenschutzbeauftragter bestellt, entfällt nach Art. 18 Abs. 2 zweiter Spiegelstrich der EG-Datenschutzrichtlinie die Pflicht, die Verfahrensbeschreibungen bei der zentralen Kontrollstelle zu melden. Dies soll allerdings nicht dazu führen, daß die Transparenz der Datenverarbeitung verlorengeht. Daher haben in diesem Fall nach Art. 21 Abs. 2 i.V.m. Art. 19 Abs. 1 der EG-Datenschutzrichtlinie die datenverarbeitenden Stellen selbst ein Verzeichnis über die bei ihnen eingesetzten automatisierten Verfahren zu führen, das die Angaben nach Abs. 1 enthalten muß. Auch dieses Verzeichnis ist im oben erwähnten Umfang für jedermann zur Einsicht bereitzuhalten. Die Führung dieses Verzeichnisses sowie die Gewährung der Einsicht obliegt der oder dem behördlichen Datenschutzbeauftragten.

Zu § 8

Absatz 1

Die Vorschrift beschreibt die Anforderungen, die speziell an gemeinsame (automatisierte) Verfahren oder an Abrufverfahren zu stellen sind.

Absatz 2

Bei beiden Verfahren haben die beteiligten Stellen die Zulässigkeit des Verfahrens zu kontrollieren und müssen in diesem Zuge bestimmte Daten schriftlich fixieren.

Absatz 3

Wenn mehrere Stellen auf einen einheitlichen Datenbestand zugreifen, muß im einzelnen nachvollzogen werden können, wann welche datenverarbeitende Stelle welche Daten erhalten hat. Zu diesem Zweck sind bei gemeinsamen Verfahren genauso wie bei automatisierten Übermittlungsverfahren sämtliche Übermittlungen zu protokollieren.

Absatz 4

Diese Vorschrift regelt die Verantwortung für die Zulässigkeit von Datenübermittlungen im Rahmen von Abrufverfahren.

Absatz 5

Hier werden Ausnahmen von den Absätzen 1 bis 4 für der Öffentlichkeit zugängliche Datenbestände festgeschrieben.

Zu § 9

Diese Vorschrift enthält die Regelung zur Vorabkontrolle und setzt damit Art. 20 der EG-Datenschutzrichtlinie um. Danach haben die Mitgliedstaaten durch nationales Recht sicherzustellen, daß bei solchen Datenverarbeitungen, die besonders dazu geeignet sind, die Rechte der Betroffenen zu gefährden, durch eine sogenannte Vorabkontrolle mögliche Rechtsbeeinträchtigungen festgestellt und ausgeschlossen werden.

Die EG-Datenschutzrichtlinie sieht vor, daß die bei den datenverarbeitenden Stellen installierten Datenschutzbeauftragten oder die jeweilige Kontrollinstanz an der Vorabkontrolle teilnehmen. Die Frist, innerhalb derer diesen Stellen Gelegenheit zur Prüfung einzuräumen ist, wird von den datenverarbeitenden Stellen bestimmt.

Zu § 10

Mit der Regelung wird die Vorgabe von Art. 18 Abs. 2 zweiter Spiegelstrich der EG-Datenschutzrichtlinie umgesetzt. Die EG-Datenschutzrichtlinie enthält in Art. 18 für den nationalen Gesetzgeber die grundsätzliche Verpflichtung, ein System der Dateimeldungen festzuschreiben, das dem bisher nach § 8 Abs. 1 LDSG a.F. durchgeführten Meldeverfahren entspricht. Ausnahmen sind insbesondere dann zulässig, wenn entweder Verarbeitungen mit geringem Risiko vorliegen oder bei der datenverarbeitenden Stelle ein Datenschutzbeauftragter bestellt wurde.

Absatz 1

Die Vorschrift eröffnet für die datenverarbeitenden Stellen die Möglichkeit der förmlichen Bestellung einer oder eines behördlichen Datenschutzbeauftragten. Satz 2 erlaubt es vor allem kleineren datenverarbeitenden Stellen, eine gemeinsame Beauftragte oder einen gemeinsamen Beauftragten zu bestellen. In diesem Fall ist sie oder er unmittelbar der Leiterin oder dem Leiter der datenverarbeitenden Stelle zu unterstellen, der sie oder er angehört (siehe auch Absatz 3).

Absatz 2

Die Bestellung einer oder eines behördlichen Datenschutzbeauftragten führt nur dann zur Befreiung von der Meldepflicht im Sinne von § 7 Abs. 5, wenn tatsächlich eine effektive Datenschutzkontrolle vor Ort gewährleistet ist. Die Absätze 2 bis 4 beschreiben deshalb die Anforderungen an die Person der oder des Beauftragten für den Datenschutz sowie an die ihnen zur Verfügung stehenden Arbeitsbedingungen. Zur erforderlichen Sachkunde gehört ein Mindestmaß an Verständnis für automatisierte Datenverarbeitung. Von Bedeutung

ist die Regelung, wonach eine Kollision mit anderen dienstlichen Aufgaben durch die Bestellung nicht hervorgerufen werden darf. Damit ist z.B. die Bestellung des Leiters der IT-Abteilung ausgeschlossen. Die Bestellung betrifft die Person der oder des Beauftragten selbst und wirkt sich möglicherweise auch auf weitere Beschäftigte aus. Aus diesem Grund unterliegt sie der Mitbestimmung nach § 51 MBG.

Wegen der der oder dem Beauftragten für den Daten schutz umfassend gewährten Kontrollrechte muß diese Funktion immer durch einen Beschäftigten der datenverarbeitenden Stelle ausgeführt werden. Private können jedoch als Sachverständige vor allem für allgemeine Fragen der Organisation der Verfahren und für technische Beratungen eingesetzt werden. Zugriff auf die personenbezogenen Daten darf externen Beraterinnen und Beratern jedoch nur im Einzelfall und nur dann gewährt werden, wenn die oder der Betroffene zugestimmt hat.

Absatz 3

Geregelt wird die Rechtsstellung der oder des behördlichen Datenschutzbeauftragten. In Art. 18 Abs. 2 zweiter Spiegelstrich der EG-Datenschutzrichtlinie wird verlangt, daß die oder der interne Datenschutzbeauftragte die „unabhängige Überwachung" der datenschutzrechtlichen Vorschriften vornimmt. Die unabhängige Stellung ist durch die insoweit vorgesehene Weisungsfreiheit gesichert. Ein Benachteiligungsverbot stärkt die Rechtsstellung der oder des Datenschutzbeauftragten. Eine effektive Wahrnehmung der Aufgaben ist der oder dem Datenschutzbeauftragten nur möglich, wenn sie oder er über die nötigen Ressourcen verfügt und vor allem in ausreichendem Umfang von anderen Aufgaben freigestellt wird. Welche Größenordnung der Freistellung erforderlich ist, hängt vom Umfang der Datenverarbeitung und des Umgangs mit personenbezogenen Daten bei der jeweiligen Stelle ab. Bei größeren öffentlichen Stellen ist daran zu denken, eine Person hauptamtlich zur oder zum Beauftragten für den Datenschutz zu bestellen. Die Möglichkeit der Anrufung der oder des behördlichen Datenschutzbeauftragten ist nicht nur für die Beschäftigten der öffentlichen Stelle, sondern für sämtliche Betroffene (§ 2 Abs. 1) eröffnet. Der oder dem Beauftragten stehen zwar grundsätzlich dieselben Einsichtsrechte zu wie der oder dem Landesbeauftragten für Datenschutz. So läßt z.B. die Vor-

schrift als Spezialregelung zu § 106 a Abs. 3 LBG auch eine Einsichtnahme in Perso-nalakten zu. Soweit allerdings spezifische Amts- und Berufsgeheimnisse nicht nur von Ärzten, sondern z.B. auch des (Haupt-)Personalrats, der Gleichstellungsbeauftragten oder der Vertrauensfrau bzw. des Vetrauensmannes der Schwerbehinderten bestehen, hat die oder der behördliche Datenschutzbeauftragte kein Einsichtsrecht. Im Interesse der Betroffenen steht ein derart weitgehendes Einsichtsrecht ausschließlich der oder dem Landesbeauftragten für Datenschutz zu (vgl. § 35 Abs. 1). Die datenverarbeitende Stelle hat der oder dem Datenschutzbeauftragten die Informationen zu liefern, die für die Führung des Verzeichnisses nach § 7 erforderlich sind.

Absatz 4

Es werden die Aufgaben der oder des behördlichen Datenschutzbeauftragten für den Datenschutz festgelegt. Wichtigste Aufgabe ist die Überwachung der Datenverarbeitung und der Einhaltung der datenschutzrechtlichen Vorschriften. Dies umfaßt die Befugnis, die Rechtmäßigkeit der Datenverarbeitung der jeweiligen Stelle zu prüfen. Daneben hat die oder der Datenschutzbeauftragte die öffentliche Stelle zu beraten und zu unterstützen, um die Einhaltung der Vorschriften zu gewährleisten. Weiterhin sind die Beschäftigten der datenverarbeitenden Stelle mit den Bestimmungen der einschlägigen Gesetze bekannt zu machen. Damit wächst der oder dem Beauftragten die bisher beim Datengeheimnis nach § 6 LDSG a.F. vorgesehene Unterrichtungspflicht zu.

Des weiteren hat sie oder er das Verzeichnis nach § 7 Abs. 1 zu führen und nach § 7 Abs. 4 für jedermann zur Einsicht bereitzuhalten. Schließlich hat sie oder er die Vorabkontrolle nach § 9 Abs. 1 durchzuführen.

Zu § 11

Absatz 1

Es wird klargestellt, daß das LDSG echte Rechtsgrundlagen für die Datenverarbeitung bereithält, was bislang zumindest umstritten war.

Absatz 2

Der Absatz enthält eine eigenständige Rechtsgrundlage für die Verarbeitung bestimmter, für das informationelle Selbstbestimmungsrecht weniger bedeutsamer Daten. Im Hinblick auf die geringe Gefährdung der Betroffenen bei Daten, die allgemein zugänglichen Quellen entnommen werden können oder die von den Betroffenen selbst zur Veröffentlichung bestimmt wurden, ist die Verarbeitung ohne weitere Voraussetzungen zulässig, soweit schutzwürdige Belange der Betroffenen nicht beeinträchtigt sind. Dies wäre z.B. dann der Fall, wenn allgemein zugängliche Daten über Betroffene in Verfahren verarbeitet wurden, die im Verhältnis zu den Betroffenen einem konkreten Zweck dienen. Nach der zweiten Alternative der Vorschrift ist die Datenverarbeitung vor allem in Büchereien und Bibliotheken unproblematisch, da in diesen Fällen die Betroffenen (Autoren) ihre Daten selbst zur Veröffentlichung bestimmt haben. Auch hier gilt als Grenze das Entgegenstehen schutzwürdiger Belange der Betroffenen. Die datenverarbeitenden Stellen haben im Zweifel den Nachweis zu führen, daß die Daten tatsächlich aus allgemein zugänglichen Quellen stammen oder von den Betroffenen zur Veröffentlichung bestimmt wurden.

Absatz 3

Die Vorschrift setzt Art. 8 der EG-Datenschutzrichtlinie um und definiert eine besondere Kategorie von Daten, deren Verarbeitung über die Anforderungen des Absatzes 1 hinaus besonderen Einschränkungen unterliegt. Diese Daten dürfen also nur dann nach Absatz 1 verarbeitet werden, wenn zugleich die hier genannten Anforderungen erfüllt sind. Die EG-Daten-schutzrichtlinie sieht vor, daß die besonders sensiblen Daten entgegen dem allgemeinen Verarbeitungsverbot dann aus Gründen eines wichtigen öffentlichen Interesses verarbeitet werden können, wenn die Mitgliedstaaten angemessene Garantien vorsehen

(Art. 8 Abs. 4 EG-Datenschutzrichtlinie). Hiervon ist in verschiedenen bereichsspezifischen Gesetzen Gebrauch gemacht worden. Daher ist die Verarbeitung der in § 11 Abs. 3 genannten Daten auf bereichsspezifischer Grundlage erlaubt. Darüber hinaus sieht die EG-Daten-schutzrichtlinie einzelne Durchbrechungen hinsichtlich der besonders geschütz-ten Daten vor. Neben der Einwilligung des Betroffenen kommen hier vor allen Dingen die in § 11 Abs. 3 Nrn. 5 und 6 genannten Fallgruppen in Betracht. Diese entsprechen Art. 8 Abs. 2 Buchstabe e der EG-Datenschutzrichtlinie. Die Ausnahme in § 11 Abs. 3 Nr. 4 entspricht der Regelung in Hessen. Sie ist richtlinienkonform, da angemessene Garantien bereits durch die Zweckbindung bewirkt werden können.

Absatz 4

Es wird zunächst die Pflicht aufgestellt, bei der Verarbeitung personenbezogener Daten dafür zu sorgen, daß eine Trennung der Daten nach Betroffenen und gegebenenfalls nach unterschiedlichen Erforderlichkeiten möglich ist. Diese Trennung ist auch Voraussetzung, um die im europäischen Recht immer weiter verbreiteten allgemeinen Informationsrechte (Aktenöffentlichkeit) ohne unzumutbaren Aufwand zu realisieren. Die Pflicht hat besondere Bedeutung hinsichtlich der Speicherung auf papierenen Datenträgern, namentlich in Akten. In elektronischer Form vorliegende Daten werden sich in der Regel technisch bedingt leichter trennen lassen.

Für den Fall, daß sich die Trennung dennoch als unmöglich oder unverhältnismäßig aufwendig erweist, verallgemeinert Satz 2 die bisher schon in § 12 Abs. 2 enthaltene Regelung über den Anwendungsfall der Übermittlung auf die anderen hier genannten Datenverarbeitungsvorgänge hinaus. Die Vorschrift regelt die Fälle, in denen in Akten mit den Daten der Betroffenen entweder Daten anderer Betroffener oder eigene Daten der Betroffenen, die für die Aufgabenerfüllung nicht erforderlich sind, in einer Weise verbunden sind, daß sich ihre Trennung gar nicht oder nur mit unverhältnismäßigem Aufwand realisieren ließe. In diesen Fällen darf ausnahmsweise auch von den nicht erforderlichen Daten Kenntnis genommen werden; sie dürfen innerhalb der datenverarbeitenden Stelle weitergegeben werden und an Dritte übermittelt werden. Voraussetzung ist allerdings zusätzlich, daß nicht schutzwürdige Interessen der Betroffenen im Einzelfall überwiegen. Da diese Art der Datenverarbeitung nur eine

Folge der „Untrennbarkeit" der Daten ist, sind die nicht erforderlichen Daten von der weiteren Verwendung ausgeschlossen. Insoweit unterliegen sie einem Verwertungsverbot.

Absatz 5

Die Vorschrift beschreibt richtlinienkonforme Ausnahmen vom Verarbeitungsverbot des Absatzes 3.

Absatz 6

Die Vorschrift enthält eine Privilegierung der Verarbeitung pseudonymisierter Daten. Bei richtiger Handhabung könnte sich die Pseudonymisierung als ein wichtiges Instrument zur Vermeidung unerfreulicher Konfliktlagen erweisen, bei denen in der Vergangenheit häufig wichtige andere Interessen wie Forschung, Planung, Statistik oder Öffentlichkeitsarbeit gegen den Datenschutz ins Feld geführt wurden und umgekehrt.

Zu § 12

Absatz 1

In Satz 1 und 3 wird der bisherige § 5 Abs. 2 LDSG wörtlich übernommen. Satz 2 ist zur Umsetzung von Art. 8 Abs. 2 Buchstabe a der EG-Datenschutzrichtlinie erforderlich.

Absatz 2

Die Vorschrift übernimmt im wesentlichen den Regelungsgehalt von § 5 Abs. 3 LDSG a.F. Die hier geregelte Aufklärung bei der Einholung der Einwilligung hat engen Bezug zur Aufklärung bei der Datenerhebung nach § 26, läßt sich aber davon abgrenzen. Die in § 5 Abs. 3 LDSG a. F. enthaltene Informationspflicht über Verwendungszweck und Empfängerkreis gehört nicht speziell zur Einholung der Einwilligung, sondern zur Erhebung bei den Betroffenen allgemein. Sie ist daher in § 26 Abs. 1 enthalten.

Absatz 3

Im Hinblick auf die wichtiger werdende Kommunikation in Rechnernetzen wird in Anlehnung an den Mediendienste-Staatsvertrag bzw. das Informations- und Kommunikationsdienstegesetz des Bundes die Möglichkeit der elektronischen Einwilligung eröffnet. Voraussetzung dafür ist ein Verfahren der digitalen Signatur, das allerdings nicht zwangsläufig den hohen Vorgaben des Signaturgesetzes entsprechen muß. Ausreichend ist es z.B., das Programm PGP einzusetzen. Abweichend von den Regelungen des Multimediarechts wurde darauf verzichtet zu verlangen, daß der Inhalt der Einwilligung jederzeit ohne unverhältnismäßigen Aufwand abgerufen werden kann. Eine solche Abrufbarkeit stellt hohe technische Anforderungen an die öffentlichen Stellen, denen vermutlich nicht in allen Bereichen genügt werden kann. Der Verzicht auf die Abrufbarkeit führt nicht zu Nachteilen für die Betroffenen, da diese auch mit Hilfe des Auskunftsanspruchs nach § 27 Informationen über die von ihnen gegebenen Einwilligungen abrufen können.

Zu § 13

In § 13 werden Regelungen zur Datenerhebung und zur Zweckbindung zusammengefaßt.

Absatz 1

Eine materielle Regelung zur Zulässigkeit speziell für die Datenerhebung ist ebenso verzichtbar wie für das Speichern, da insoweit die Grundsätze des § 11 Absätze 2 und 3 gelten. Satz 1 enthält daher nur Vorgaben für die Art und Weise der Erhebung. Er stellt den Grundsatz auf, daß Daten bei den Betroffenen und mit ihrer Kenntnis zu erheben sind. Die Durchbrechungen dieses Grundsatzes in Satz 2 entsprechen im wesentlichen dem bisherigen § 10 Abs. 4 Satz 1 LDSG. Auf die Pflicht zur Benachrichtigung der oder des Betroffenen konnte an dieser Stelle zunächst verzichtet werden. Die entsprechenden Regelungen finden sich nunmehr in § 28.

Absatz 2

Wie im bisherigen § 9 LDSG wird der Grundsatz der Zweckbindung aufgestellt. Damit wird zum einen die zweckändernde Verarbeitung vorbehaltlich der in Abs. 3 definierten Ausnahmen ausgeschlossen. Zum anderen wird die materielle Zulässigkeit der weiteren Verarbeitung dahingehend präzisiert, daß nur bei rechtmäßiger Erhebung bzw. erster Speicherung die weitere Verarbeitung zum selben Zweck im Rahmen der Erforderlichkeit für die rechtmäßige Aufgabenerfüllung erlaubt ist. Damit ist klargestellt, daß Daten, die unrechtmäßig erhoben oder erstmalig gespeichert wurden, selbst dann nicht weiterverarbeitet werden dürfen, wenn die weitere Verarbeitung zur rechtmäßigen Aufgabenerfüllung erforderlich sein sollte.

Absatz 3

Es werden die Fälle benannt, in denen die Zweckänderung entgegen dem Grundsatz des Abs. 2 erlaubt ist. Dies ist zunächst der Fall, wenn die Einwilligung der oder des Betroffenen vorliegt. Weiter ist die Zweckänderung nach Nr. 1 dann unproblematisch, wenn sie auf eine spezielle Erlaubnisnorm gestützt werden kann. Dies muß eine bereichsspezifische Erlaubnisnorm sein. Die in § 9 Abs. 2 Nr. 1 LDSG a.F. noch bestehende zweite Alternative („wenn eine Rechtsvorschrift dies (...) im Einzelfall zwingend voraussetzt") muß entfallen, da über 15 Jahre nach Erlaß des Volkszählungsurteils Zweckänderungen auf bereichsspezifische Regelungen gestützt werden müssen. Nr. 2 läßt die Zweck-

änderung zur Abwehr von erheblichen Nachteilen für das Allgemeinwohl, zur Abwehr von Gefahren für bestimmte hochrangige Rechtsgüter und zur Abwehr schwerwiegender Beeinträchtigungen anderer Rechtsgüter einzelner zu.

Die damit verbundene Erleichterung der Zweckänderung trägt der Erkenntnis Rechnung, daß das Recht auf informationelle Selbstbestimmung im Einzelfall auch hinter anderen als den bisher in § 9 Abs. 2 Nr. 2 LDSG a.F. genannten Rechtsgütern zurücktreten muß. Im Einzelfall können zum Beispiel auch Gefährdungen des Eigentums oder anderer vermögenswerter Interessen Vorrang vor dem informationellen Selbstbestimmungsrecht haben. Voraussetzung ist aber in diesen Fällen eine schwerwiegende Beeinträchtigung. Mit dieser Formulierung sollen bloße Bagatellbeeinträchtigungen ausgeschlossen werden.

In Nr. 3 wurde zur Vereinfachung der Normanwendung auf den 2. Teilsatz verzichtet. Schon bisher dürfte die Gebotenheit der Zweckdurchbrechung für die Verfolgung der Straftaten oder Ordnungswidrigkeiten in der Praxis regelmäßig bejaht worden sein.

In Nr. 4 wurde der erste Teilsatz hinzugefügt um zu verdeutlichen, daß vor der Inanspruchnahme der Ausnahmebefugnis der mutmaßlichen Einwilligung der Versuch gemacht werden muß, die tatsächliche Einwilligung der oder des Betroffenen einzuholen.

Absatz 4

Die Vorschrift trägt wiederum Art. 8 der EG-Datenschutzrichtlinie Rechnung und beschränkt die Verarbeitung der in § 11 Abs. 3 Satz 1 beschriebenen besonders sensiblen Daten für andere Zwecke in den Fällen, in denen keine Einwilligung der Betroffenen vorliegt. Wie schon im Falle des § 11 Abs. 3 (s. § 11 Abs. 5) bestehen jedoch auch hier richtlinienkonforme Ausnahmen von dieser Einschränkung.

Absatz 5

Zum besseren Schutz der in der Ausbildung und Prüfung verwendeten Daten wurde neu die Pflicht aufgenommen, die zu diesen Zwecken verwendeten Daten nach Möglichkeit zu anonymisieren oder wenigstens zu pseudonymisieren. Die Inanspruchnahme der Zweckänderungsbefugnis des Abs. 4 Satz 2 setzt daher nunmehr voraus, daß zunächst die Möglichkeit der Anonymisierung oder Pseudonymisierung geprüft wird.

Absatz 6

Die besondere Zweckbindung ergreift nicht nur die bei Maßnahmen zur Datensicherheit anfallenden Daten wie z.B. Protokolldateien. Sie gilt auch für die Daten, die im Rahmen der datenschutzrechtlichen Prüfungen durch die behördlichen Datenschutzbeauftragten nach § 10 und durch die oder den Landesbeauftragten für Datenschutz verarbeitet werden.

Absatz 7

Die Regelung entspricht dem bisherigen § 12 Abs. 4 LDSG. Wegen des Regelungszusammenhangs wurde er bei den Vorschriften der Zweckbindung aufgenommen.

Zu § 14

Absatz 1

Die Regelung entspricht § 12 Abs. 1 a. F.

Absatz 2

Die Vorschrift regelt die Verantwortlichkeiten bei der Datenübermittlung zwischen öffentlichen Stellen. Sie bringt zum einen eine sprachliche Verein

fachung der bisher in § 12 Abs. 3 a.F. enthaltenen Regelung. Außerdem wird die Verantwortlichkeit klarer zwischen den beteiligten Stellen verteilt.

Die bisher in § 12 Abs. 2 und 4 a.F. enthaltenen Regelungen finden sich nunmehr in § 11 Abs. 4 bzw. § 13 Abs. 7.

Zu § 15

Absatz 1

Die bisherige Regelung des § 15 Abs. 1 LDSG konnte zur Folge haben, daß die Übermittlung in den nicht-öffentlichen Bereich unter leichteren Voraussetzungen möglich war als die zwischen öffentlichen Stellen. Um dieses offenkundige und sachwidrige Ungleichgewicht der Regelungen zu beseitigen, wurde Nummer 1 neu gefaßt und in Nummer 2 die Befugnis geschaffen, auch in den Fällen an nicht-öffentliche Stellen zu übermitteln, in denen diese Übermittlung zur rechtmäßigen Aufgabenerfüllung der übermittelnden Stelle erforderlich ist.

Absatz 2

Die Vorschrift ist gegenüber § 15 Abs. 2 LDSG a.F. unverändert geblieben.

Zu § 16

Mit § 16 werden Art. 25 und 26 der EG-Datenschutzrichtlinie umgesetzt.

Absatz 1

Die EG-Datenschutzrichtlinie verfolgt das Ziel, den Datenverkehr innerhalb der Europäischen Union zu vereinfachen. Zu diesem Zweck wird ein einheitliches Datenschutzniveau in den Mitgliedstaaten geschaffen. Ist dieses einheitliche Niveau erreicht, so darf die Datenübermittlung an die öffentlichen und nicht-öffentlichen Stellen der anderen Mitgliedstaaten nicht an höhere Voraussetzungen geknüpft werden als für Übermittlungen im Mitgliedstaat selbst. Dem trägt Satz 1 Rechnung. Als Voraussetzung für die Übermittlung an Stellen in Drittstaaten schreibt Art. 25 der EG-Datenschutzrichtlinie vor, daß dort ein „an-

ge-messenes Schutzniveau gewährleistet" sein muß. Dies muß von der übermittelnden Stelle selbst beachtet werden. Die Angemessenheit oder ihr Fehlen können aber auch in einem von der EG-Datenschutzrichtlinie festgelegten Verfahren durch die Europäische Kommission festgestellt werde. Die Mitgliedstaaten haben die aufgrund der Feststellungen der Kommission gebotenen Maßnahmen zu treffen; d.h. sie haben vor allem dafür zu sorgen, daß beim Fehlen des angemessenen Schutzniveaus keine Datenübermittlungen in diese Länder stattfinden. Für die Regelungsebene des LDSG bedeutet dies, daß die datenverarbeitenden Stellen grundsätzlich zunächst selbst über die Angemessenheit des Schutzniveaus befinden.

Absatz 2

Eine Übermittlung kommt auch in den in Art. 26 der EG-Datenschutzrichtlinie genannten Ausnahmetatbeständen in Betracht. Diese werden in Absatz 2 nachvollzogen.

Absatz 3

Da die Entscheidungen nach den Absätzen 1 und 2 nicht leicht zu treffen sind, muß hierzu die oder der Landesbeauftragte für Datenschutz gehört werden.

Absatz 4

Mit dieser Regelung soll erreicht werden, daß die Zweckbindung auch nach der Übermittlung ins Ausland aufrechterhalten wird.

Zu § 17

Absätze 1 bis 3

Die Regelungen des bisherigen § 4 Abs. 1 bis 3 LDSG werden übernommen. Allerdings war in Abs. 1 als neuer Satz 3 die Klarstellung erforderlich, daß die Weitergabe von Daten an Auftragsdatenverarbeiter keine Übermittlung im Sinne dieses Gesetzes darstellt. Eine entsprechende Regelung fand sich bisher in der Definition des Dritten in § 2 Abs. 4 LDSG a.F. Nach dem Verzicht auf diese Definition war die entsprechende Regelung in die speziellen Vorschriften zu den Auftragsdatenverarbeitern aufzunehmen.

Absatz 4

Bisher war im datenschutzrechtlichen Schrifttum umstritten, ob das Erbringen von Wartungsarbeiten an EDV-Anlagen oder von vergleichbaren Dienstleistungen bei der Datenverarbeitung als Auftragsdatenverarbeitung angesehen werden kann. Häufig wurde diese Frage nur bejaht, um die Rechtsfolgen der Auftragsdatenverarbeitung auch auf die genannten Dienstleistungsarbeiten anwenden zu können. In der Praxis kam es immer wieder zu Unsicherheiten über die rechtlichen Rahmenbedingungen für Wartungsarbeiten durch Externe. Zur Klarstellung wurde nunmehr in Abs. 4 die Bestimmung aufgenommen, daß die Erbringung von Wartungsarbeiten wie die Auftragsdatenverarbeitung behandelt wird. Auch diese Dienstleister müssen sorgfältig ausgewählt und überwacht werden. Bei ihrer Tätigkeit müssen sie sich den durch die datenverarbeitenden Stellen veranlaßten Kontrollen unterwerfen.

Absatz 5

Ein datenschutzrechtliches Problem besteht in der zunehmenden Einbeziehung solcher Dritter bei der Datenverarbeitung der öffentlichen Stellen, die aufgrund ihres eigenen Entscheidungsspielraums und besonderer Sachkenntnisse nicht als Auftragsdatenverarbeiter angesehen werden können. Für diesen Fall trifft Absatz 5 besondere Regelungen. Dabei ist Absatz 5 als Rechtsgrundlage für Datenübermittlungen formuliert. Voraussetzung für die Zulässigkeit der Übermittlung ist, daß die Auftragnehmer beratend oder gutachterlich tätig werden. Die Auftragnehmer sind durch die übermittelnde Stelle zur Zweckbindung und zur Rückgabe bzw. Löschung der verwendeten Daten zu verpflichten. Die letztgenannte Pflicht kann allerdings dadurch modifiziert sein, daß standesrechtliche Sonderregelungen eine Aufbewahrung bestimmter Daten vorsehen. Im übrigen sind die Sorgfalts- und Überwachungsmaßstäbe anzulegen, die auch für die Einschaltung von Auftragsdatenverarbeitern nach den Abs. 1 bis 3 zu beachten sind. Die entsprechende Anwendung von Abs. 1 hat zur Folge, daß die öffentlichen Stellen zwar für die Datenverarbeitung verantwortlich bleiben und die Rechte der Betroffenen bei ihnen geltend zu machen sind. Da jedoch der Gesetzgeber des LDSG keine Zuständigkeit für die Regelung der Rechtsverhältnisse bei den in Abs. 5 Satz 1 genannten Personen hat, wird damit nicht die Datenverarbeitung bei den auftragnehmenden Stellen geregelt. Diese bleiben vielmehr nach speziellen Rechtsvorschriften oder dem BDSG ihrerseits den Betroffenen verantwortlich für die Datenverarbeitung; die Rechte des BDSG können auch unmittelbar ihnen gegenüber geltend gemacht werden.

Zu § 18

Die Vorschrift ist eine Reaktion auf neue technische Entwicklungen. Ziel ist es, die Rechte der Betroffenen auch unter diesen Bedingungen angemessen zu gewährleisten.

Die Vorschrift sieht im übrigen keine Bestimmungen dazu vor, welche Stelle als datenverarbeitende Stelle anzusehen ist, ob mit der Ausgabe der Systeme Vorteile verbunden werden dürfen oder ob biometrische Merkmale mitgespeichert werden dürfen. Die datenschutzrechtliche Erfahrung mit dieser Technologie ist bisher noch nicht soweit gediehen ist, daß diesbezüglich bereits

eine Regelung getroffen werden könnte.

Absatz 1

Mit den mobilen Datenverarbeitungssystemen werden nach dem heutigen Stand der Technik vor allem Chipkarten erfaßt. Allerdings sind heute schon Entwicklungen absehbar, bei denen der Chip nicht länger in Form einer Karte angewandt wird. Auch ist der Chip keine zwingende Voraussetzung für mobile Speichertechniken. Aus diesem Grunde kann nicht auf den Begriff Chipkarte abgestellt werden. Von der Legaldefinition sollen vielmehr folgende Merkmale erfaßt werden:

- Die Systeme werden von einer Stelle an die Betroffenen ausgegeben.

- Es existieren Schnittstellen, die von der ausgebenden Stelle oder von Dritten bereitgestellt werden.

- Über diese Schnittstellen können Daten automatisiert ausgetauscht werden; dazu gehört auch, daß durch den Datenaustausch Datenverarbeitungen auf den mobilen oder den stationären Systemen angestoßen werden.

Derartige Systeme bringen besondere Gefährdungen für die Rechte der Betroffenen mit sich. Ihnen ist es regelmäßig nicht möglich, selbst festzustellen, was in den Datenverarbeitungssystemen gespeichert wird. Bereits heute existieren Anwendungen, bei denen die Betroffenen nicht bemerken können, daß ein Datenaustausch zwischen den mobilen Systemen und einer Schnittstelle stattfindet. Zu denken ist hier z.B. an kontaktlose Chipkarten. Aufgrund dieser besonderen Gefährdungslage sind besondere Schutzvorschriften erforderlich. Daher dürfen entsprechende Systeme nur mit der Einwilligung der oder des Betroffenen oder aufgrund einer Rechtsvorschrift eingesetzt werden. Als Rechtsvorschrift i.S.d. § 18 sind auch Regelungen in arbeitsrechtlichen oder dienstrechtlichen Kollektivvereinbarungen anzusehen.

Absatz 2

Bei mobilen Verarbeitungssystemen ist die mangelnde Transparenz für die Be-

troffenen besonders riskant. Daher ordnet die Vorschrift an, daß die ausgebende Stelle die Transparenz sicherzustellen hat. Es muß für die oder den Betroffenen jederzeit erkennbar sein, ob Datenverarbeitungsvorgänge stattfinden, welche Daten dabei verarbeitet werden und welcher Verarbeitungsvorgang im einzelnen abläuft.

Absatz 3

Die Aufklärung über die Rechte der Betroffenen hat in diesem Sonderfall nicht erst bei der ersten Datenverarbeitung mit oder auf dem System, sondern bereits bei Ausgabe des Systems (also z.B. bei der Aushändigung der Chipkarte) zu erfolgen.

Zu § 19

§ 19 setzt Art. 15 der EG-Datenschutzrichtlinie um. Danach ist es verboten, Personen für sie nachteiligen Entscheidungen zu unterwerfen, bei denen einzelne Aspekte ihrer Person automatisiert bewertet werden. Eine entsprechende Vorschrift findet sich bereits in § 106 g Abs. 4 Landesbeamtengesetz für den dortigen Anwendungsbereich. Ausnahmen sieht die EG-Datenschutzrichtlinie vor, wenn ein Gesetz angemessene Garantien zur Wahrung der Rechte der Betroffenen enthält oder den Betroffenen die Möglichkeit eingeräumt wird, ihre persönlichen Interessen geltend zu machen. Letzteres ist bereits im Zuge der jeweiligen Gesetzgebung zu berücksichtigen, da andernfalls Verhältnismäßigkeitsgrundsätze nicht beachtet würden. Andernfalls käme auch die jeweilige öffentliche Stelle in die Situation, die Rechtmäßigkeit einer Vorschrift überprüfen zu müssen. Voraussetzung für das Verbot automatisierter Einzelentscheidungen ist, daß mehrere Informationen über den Betroffenen zusammengeführt werden und einer Bewertung unterzogen werden.

Zu § 20

Die Vorschrift übernimmt in wesentlichen Teilen Regelungen des bisherigen § 32 LDSG. Zusätzlich wurde eine Aufbewahrungsfrist für gespeicherte Bilder von im Regelfall sieben Tagen mit den erforderlichen Ausnahmemöglichkeiten verankert. Die in den bereichsspezifischen Normen für die Polizei und den Verfassungsschutz enthaltenen Rechtsgrundlagen zur Videoüberwachung und -aufzeichnung bleiben unberührt.

Zu § 21

Die Vorschrift geht auf den bisherigen § 31 LDSG zurück. Sie wurde stark vereinfacht und auf ihren wesentlichen Gehalt reduziert. Bereits aus den allgemeinen Vorschriften über die Unterrichtung bei der Einholung der Einwilligung und bei der Datenerhebung ergibt sich, daß die oder der Betroffene vollständig über Verwendungszweck, Art, Umfang und Zeitraum des Einsatzes des Fernmeßdienstes zu unterrichten ist. Entsprechendes gilt für Fernwirkdienste. Auch auf eine besondere Vorschrift zur Zweckbindung konnte verzichtet werden, da insoweit die allgemeine Zweckbindungsvorschrift nach § 13 Abs. 2 bis 6 Platz greift.

Zu § 22

Die Vorschrift stellt eine bereichsspezifische Rechtsgrundlage für die Datenverarbeitung zu wissenschaftlichen Zwecke dar. Die Änderungen im Vergleich zum bisherigen § 28 LDSG zielen vor allem darauf ab, die Stellen, die zu wissenschaftlichen Zwecken Daten verarbeiten, noch stärker als bisher zum Anonymisieren oder wenigstens Pseudonymisieren der Daten zu veranlassen. Dadurch sollen Konflikte zwischen den datenschutzrechtlichen und den Forschungsbelangen möglichst von vornherein vermieden und im Ergebnis die wissenschaftliche Forschung erleichtert werden.

Absatz 1

Die Vorschrift stellt die Verpflichtung auf, die Daten, die für wissenschaftliche Zwecke verarbeitet oder übermittelt werden sollen, im Regelfall zu anonymisieren. Nur wenn besondere Gründe dafür vorliegen, kann hiervon ausnahmsweise abgesehen werden. Nach der Anonymisierung liegen keine personenbezogenen Daten mehr vor. In diesen Fällen ist daher die Verarbeitung zu wissenschaftlichen Zwecken keinerlei weiteren Beschränkungen unterworfen.

Für den Fall, daß die Anonymisierung nicht möglich ist, sieht Satz 2 als zweite Stufe eine Pseudonymisierung der Daten vor. Die pseudonymisierten Daten werden im Ergebnis genauso behandelt wie solche, die anonymisiert wurden. Dies ist gerechtfertigt, da bei fehlendem Zugriff auf die Zuordnungsfunktion von den pseudonymisierten Daten keine wesentlich größere Gefährdung für das Persönlichkeitsrecht ausgeht als von anonymisierten Daten.

Absatz 2

In der Praxis hat sich häufig das Problem ergeben, daß die Forschung betreibende Stelle zwar bereit und in der Lage war, mit anonymisierten oder pseudonymisierten Daten zu arbeiten, jedoch bei der Stelle, die sich im Besitz der Daten befand, nicht genügend Ressourcen zur Verfügung standen, um die Anonymisierung oder Pseudonymisierung durchzuführen. In der Folge wurden dann die Daten oft auf der Grundlage einer Genehmigung der Aufsichtsbehörde ohne Anonymisierung oder Pseudonymisierung übermittelt. Um mangelnde Ressourcen künftig nicht mehr zu einem datenschutzrechtlichen Nachteil für die Betroffenen werden zu lassen, ist vorgesehen, daß in diesen Fällen die Anonymisierung oder Pseudonymisierung auch durch die mit der Forschung befaßten Personen erfolgen kann. Voraussetzung ist allerdings, daß die Forschung Betreibenden zuvor nach dem Verpflichtungsgesetz vom 2. März 1974 (BGBl. I S. 469, 547), geändert durch Gesetz vom 15. August 1974 (BGBl. I S. 1942) zur Verschwiegenheit verpflichtet wurden. Nachdem durch die Forscher selbst die Pseudonymisierung durchgeführt wurde, muß diesen selbstverständlich der Zugriff auf die Zuordnungsfunktion verwehrt werden.

Absatz 3

Ist weder ein Anonymisieren noch ein Pseudonymisieren möglich, kann die Datenverarbeitung in den hier abschließend aufgezählten Fallkonstellationen ausnahmsweise dennoch zulässig sein.

Absatz 4

Die Genehmigung nach Abs. 3 Nr. 3 wird erteilt, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens erheblich stärker wiegt als die schutzwürdigen Belange der Betroffenen und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Diese Vorschrift soll bei Vorliegen aller weiteren Voraussetzungen wichtige Forschungsvorhaben im Einzelfall auch dann ermöglichen, wenn eine Anonymisierung oder Pseudonymisierung der Daten nicht möglich ist, aber auch die Einwilligung der oder des Betroffenen nicht oder nur mit unverhältnismäßigem Aufwand eingeholt werden kann. Die Genehmigung muß inhaltlich konkretisiert sein und der oder dem Landesbeauftragten für Datenschutz mitgeteilt werden.

Absätze 5 bis 7

Die Regelungen des bisherigen § 28 LDSG Abs. 5 bis 8 wurden ohne wesentliche Änderungen übernommen.

Zu § 23

Absatz 1 entspricht dem bisherigen § 30 Abs. 1 LDSG, Absatz 2 entspricht § 30 Abs. 3 LDSG a. F. Der bisherige § 30 Absatz 2 LDSG war verzichtbar. Die Verpflichtung zum Löschen bzw. zur Sperrung ergibt sich bereits aus den allgemeinen Vorschriften.

Zu § 24

Die Regelung entspricht inhaltlich dem bisherigen § 29 LDSG.

Zu § 25

Die Vorschrift ist nahezu wortgleich mit dem bisherigen § 29 a LDSG.

Zu § 26

Die Vorschrift faßt Regelungen zusammen, die bisher in § 10 Abs. 2 und Abs. 4 LDSG a. F. enthalten waren.

Absatz 1

Der Katalog der Informationen, die der oder dem Betroffenen bei einer offenen Datenerhebung mitzuteilen sind, ist durch Art. 10 der EG-Datenschutzrichtlinie vorgegeben.

Absatz 2

Mit den Ziffern 1 bis 5 wird von der Möglichkeit des Art. 13 der EG-Datenschutzrichtlinie Gebrauch gemacht, bestimmte Behörden bei ihrer Aufgabenerfüllung von den zuvor beschriebenen Pflichten zu entbinden.

Absatz 3

Hier wird der Fall geregelt, daß Daten ohne Kenntnis der oder des Betroffenen erhoben wurden. Außerhalb der speziellen Befugnisse von Polizei und Sicherheitsbehörden kommt es zu „verdeckten" Erhebungen vor allem dann, wenn die Daten von einer anderen Stelle an die die Daten erhebende Stelle übermittelt werden. Der oder dem Betroffenen sind in diesem Falle grundsätzlich dieselben Informationen wie nach Abs. 1 zuzuleiten; verzichtet werden kann naturgemäß auf die Angabe nach Abs. 1 Nr. 4. Entsprechend Art. 11 Absatz 2 der EG-Datenschutzrichtlinie kann unter engen Voraussetzungen jedoch auf die nachträgliche Benachrichtigung der Betroffenen verzichtet werden.

Zu § 27

Absatz 1

Die Vorschrift verpflichtet die öffentlichen Stellen zur Auskunft an die Betroffenen über bestimmte Daten. Der Datenkatalog wurde in Umsetzung von Art. 12 der EG-Datenschutzrichtlinie gegenüber dem bisherigen § 18 Abs. 1 LDSG erweitert.

Auf Satz 3 der alten Regelung konnte verzichtet werden, da diese sich bereits aus allgemeinen verwaltungsrechtlichen Grundsätzen ergibt. Die Einschränkung des bisherigen § 18 Abs. 2 LDSG ist gleichfalls entfallen, da diese nicht zu begründen ist.

Absätze 2, 3 und 4

Die Regelungen entsprechen inhaltlich dem Absatz 3 bzw. den Absätzen 4 und 5 des bisherigen § 18 LDSG. Die Rechtsposition der Betroffenen wird gegenüber den bisherigen Regelungen nicht verändert.

Zu § 28

Absatz 1

Die Vorschrift enthält den Grundsatz der Berichtigung unrichtiger Daten. Auf die Regelungen des bisherigen § 19 Absatz 1 Satz 2 und 3 LDSG konnte verzichtet werden. Inwieweit Fehler in der Datenhaltung im nachhinein erkennbar sein müssen, ergibt sich schon aus den allgemeinen Anforderungen an die Aktenführung.

Absatz 2

Im Gegensatz zur bisherigen Regelung des § 19 LDSG wird nun schon im zweiten Absatz die Löschung und erst dritten Absatz die Sperrung geregelt. Dadurch wird die Sperrung von Daten deutlicher als Sondertatbestand gegenüber der Löschung erkennbar. Wie schon nach dem bisherigen § 19 Abs. 3 LDSG tritt die Pflicht zur Löschung dann ein, wenn die Speicherung entweder von Anfang an unzulässig war oder wenn sie zwar zulässig war, die Daten aber inzwischen zur Aufgabenerfüllung nicht mehr erforderlich sind. Deutlicher als bisher schreibt Satz 2 vor, daß die datenverarbeitenden Stellen selbst Regelungen darüber treffen müssen, in welchem Zeitraum die Daten als erforderlich zur Aufgabenerfüllung angesehen werden. Die Festlegung soll sich am Normalfall der Datenverarbeitung orientieren.

Absatz 3

Deutlicher als in der Regelung des bisherigen § 19 Abs. 2 LDSG werden hier die verschiedenen Konstellationen aufgezeigt, in denen die Sperrung an die Stelle der Löschung tritt. Dies ist zum einen wie bisher schon die Konstellation, daß die Richtigkeit der Daten umstritten und nicht beweisbar ist (Nr. 1). Zum anderen gehören nun die Fallgruppen der Nr. 2 bis 5 dazu. Im Falle der Nr. 4 beeinträchtigt die Löschung die Betroffene oder den Betroffenen in der Verfolgung ihrer oder seiner Rechte oder schutzwürdigen Belange z.B. dann, wenn bekannt ist, daß die oder der Betroffene vorhat, Klage zu erheben oder Schadensersatz zu fordern.

Absatz 4

In Anlehnung an den bisherigen § 19 Abs. 2 Sätze 3 und 4 LDSG wird die Rechtsfolge der Sperrung von Daten beschrieben. Weiterhin werden die Ausnahmen geregelt, in denen eine Verarbeitung oder Nutzung trotz Sperrung zulässig ist.

Absatz 5

Die Vorschrift enthält die bisher in § 20 LDSG normierte sogenannte Nachberichtspflicht. Diese war wegen Art. 12 Buchstabe c der EG-Datenschutzrichtlinie beizubehalten.

Zu § 29

Mit § 29 wird Art. 14 Buchstabe a der EG-Datenschutzrichtlinie - mit den richtlinienkonformen Einschränkungen des Absatz 2 - umgesetzt. Die Vorschrift erfaßt Konstellationen, in denen die Datenverarbeitung zwar grundsätzlich rechtmäßig und zulässig ist, sie jedoch wegen besonderer, in der jeweiligen Person begründeter Umstände die schutzwürdigen Interessen der Betroffenen in grundrechtsrelevanter Weise berühren würde. Zu denken ist beispielsweise an den Fall, daß eine amtsärztliche Untersuchung rechtmäßig angeordnet wird, die oder der Betroffene jedoch einwendet, die Person, die ihn untersuchen soll, gehöre zu seinem persönlichen Bekanntenkreis. In solchen Fällen muß es für die Betroffene oder den Betroffenen die Möglichkeit geben, wegen der besonderen persönlichen Gründe einen Einwand gegen die vorgesehene Datenverarbeitung zu erheben, auch wenn keine Befangenheit im Sinne des Verwaltungsverfahrensrechts vorliegt. Die Stelle, der gegenüber der Einwand erhoben wird, hat darüber zu befinden, ob im Einzelfall das Interesse der oder des Betroffenen überwiegt.

Zu § 30

Die Regelungen über den Schadensersatz sind inhaltlich unverändert geblieben. Im übrigen ist die Vorschrift redaktionell überarbeitet worden. So waren die Absätze 5 und 6 des bisherigen § 21 LDSG verzichtbar, da sie lediglich Fragen des Innenausgleichs zwischen mehreren Schädigern nach allgemeinen Rechtsgrundsätzen geregelt haben.

Zu § 31

Mit dieser Vorschrift wird klargestellt, daß die gesetzlich fixierten Rechte der Betroffenen nicht vertraglich ausgeschlossen werden können.

Zu § 32

(der Inhalt der Vorschrift wird sich aus einem der Novellierung vorgeschalteten Änderungsgesetz zum geltenden LDSG - Stichwort: Neuorganisation des Datenschutzes - ergeben. Die Ausgestaltung ist von der Entscheidung des Landtags abhängig, ob die oder der Landesbeauftragte für Datenschutz als oberste Landesbehörde oder als Anstalt des öffentlichen Rechts errichtet werden soll.)

Zu § 33

(der genaue Wortlaut der Vorschrift wird sich aus einem der Novellierung vorgeschalteten Änderungsgesetz zum geltenden LDSG - Stichwort: Neuorganisation des Datenschutzes - ergeben. Insofern hat auch die nachfolgende Begründung noch vorläufigen Charakter.)

Die Aufgaben der oder des Landesbeauftragten für Datenschutz werden zunächst allgemein beschrieben. In den nachfolgenden Vorschriften wird dann zwischen Kontroll- bzw. Beratungs- und Serviceaufgaben unterschieden.

Absatz 1

Die Sätze 1 und 3 (?) entsprechen dem bisherigen § 23 Abs. 1 Sätze 1 und 4 LDSG.

Absatz 2

Zukünftig nimmt die oder der Landesbeauftragte für Datenschutz auch die bisher im Innenministerium angesiedelten Aufgaben der zuständigen Aufsichtsbehörde nach § 38 BDSG wahr. Da sie oder er insoweit Exekutivfunktionen wahrnimmt, untersteht sie oder er insoweit der Rechtsaufsicht des fachlich zuständigen Innenministeriums.

Absatz 3

Satz 1 entspricht § 23 Abs. 2 Satz 1 LDSG a.F.; Satz 2 entspricht § 23 Abs. 3 Satz 2 LDSG a.F.

Zu § 34

§ 34 entspricht weitgehend dem bisherigen § 26 LDSG. Allerdings sind Eingaben nicht mehr auf die Geltendmachung der Verletzung eigener Rechte beschränkt, sondern die Petenten können sich auch dann an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz wenden, wenn sie Mißstände bei der Datenverarbeitung annehmen, von denen sie nicht selbst betroffen sind.

Zu § 35

§ 35 beschreibt die Kontrollaufgaben der oder des Landesbeauftragten für Datenschutz.

Die Regelungen der Absätze 1 und 2 entsprechen mit geringfügigen redaktionellen Änderungen dem bisherigen § 27 Absätze 1 und 2 LDSG. Dem Absatz 1 ist mit Satz 3 die ausdrückliche Befugnis der oder des Landesbeauftragten für Datenschutz zur Datenverarbeitung im Rahmen von datenschutzrechtlichen Prüfungen hinzugefügt worden. Die dabei verarbeiteten Daten unterliegen nach § 13 Abs. 6 einer absoluten Zweckbindung.

Zu § 36

Bei der Datenschutzkontrolle im öffentlichen Bereich bleiben die Instrumente der Mängelrüge und der förmlichen Beanstandung erhalten.

Absatz 1

Abgesehen von redaktionellen Änderungen entspricht Absatz 1 dem bisherigen § 25 Abs. 1 LDSG.

Absatz 2

Die Vorschrift entspricht mit geringfügigen Änderungen dem bisherigen § 25 Abs. 2 LDSG. Die nach bisherigem Recht zwingende Aufforderung der beanstandeten Stelle zur Stellungnahme und die Benachrichtigung der für diese zuständigen Aufsichtsbehörde hat sich allerdings nicht in allen Fällen als sinnvoll erwiesen. Beide Maßnahmen werden daher nun in das Ermessen der oder des Landesbeauftragten für Datenschutz gestellt.

Absätze 3 und 4

Die Absätze 3 und 4 entsprechen mit redaktionellen Änderungen den bisherigen § 25 Abs. 3 bzw. § 25 Abs. 5. § 25 Abs. 4 a.F. wurde ersatzlos gestrichen.

Zu § 37

Zwar stellt die Kontrolle der Einhaltung der datenschutzrechtliche Vorschriften weiterhin eine wichtige Aufgabe dar. Die Mitarbeiterinnen und Mitarbeiter der oder des Landesbeauftragten für den Datenschutz haben allerdings schon in der Vergangenheit zunehmend Zeit für die Beratung der datenverarbeitenden Stellen und der Bürgerinnen und Bürger verwendet. Die gesetzliche Regelung vollzieht diese Entwicklung nach und schreibt sie zugleich fest. Dahinter steht der Gedanke, daß für das Anliegen des Datenschutzes durch Überzeugung und Aufklärung im Vorfeld häufig mehr erreicht werden kann als durch die nachträgliche Verhängung von Sanktionen.

Absatz 1

Dementsprechend hat die oder der Landesbeauftragte für Datenschutz die Aufgabe, die öffentlichen Stellen in allen datenschutzrechtlichen Fragen zu beraten. Satz 1 und Satz 2 entsprechen dem bisherigen § 23 Abs. 1 Satz 2 und 3 LDSG. Satz 3 enthält die bisher in § 23 Abs. 3 Satz 1 LDSG geregelte besondere Beratungsverpflichtung gegenüber dem Landtag, den Fraktionen des Landtages und der Landesregierung.

Absatz 2

Zu den Serviceaufgaben der oder des Landesbeauftragten für Datenschutz gegenüber den Bürgerinnen und Bürgern gehört zunächst die Beratung über die Rechte der Betroffenen. In den Mittelpunkt des Interesses der Bürgerinnen und Bürger rückt aber gerade im Bereich der modernen Kommunikationsmedien zunehmend auch die

Frage, welche technischen Möglichkeiten den Betroffenen offenstehen, um sich vor unbefugtem Zugriff auf die eigenen Daten und dem Ausspioniertwerden durch Dritte zu schützen. Durch Beratung und Information auch auf diesem Gebiet werden die Chancen für einen effektiven Selbstdatenschutz verbessert.

Absatz 3

Den öffentlichen Stellen wird die Möglichkeit eröffnet, vor dem Einsatz automatisierter Verfahren ihr Datenschutzkonzept und dessen Implementierung vor Ort durch die Landesbeauftragte oder den Landesbeauftragten für Datenschutz beurteilen zu lassen. Dieses Auditing-Verfahren gibt den öffentlichen Stellen die Sicherheit, vom Konzept her für eine rechtmäßige Datenverarbeitung gesorgt zu haben. Spätere Kontrollen durch die oder den Landesbeauftragten für Datenschutz werden dadurch jedoch nicht ausgeschlossen, da der positive Ausgang des Datenschutz-Audits nur eine Momentaufnahme wiedergibt. Die Ausgestaltung des Datenschutz-Audits wird durch Verordnung geregelt.

Absatz 4

Wie bisher schon im öffentlichen Bereich üblich, wird die oder Landesbeauftragte für Datenschutz zukünftig Beratungen und Fortbildungsveranstaltungen auf Wunsch auch im nichtöffentlichen Bereich durchführen.

Absatz 5

Entsprechend dem Servicecharakter der in Abs. 3 und Abs. 4 dargestellten Aufgaben soll hierfür ein angemessenes Entgelt erhoben werden können.

Zu § 38

Im Sinne einer Entkriminalisierung wird auf die Strafnorm des bisherigen § 33 LDSG verzichtet. Sie hatte ohnehin kaum praktische Bedeutung.

§ 38 entspricht im wesentlichen § 34 LDSG a.F. Die Neufassung des Absatzes 1 Satz 2 ist notwendig, weil die Verarbeitung anonymisierter oder pseudonymisierter Daten im Gesetz verschiedentlich erleichtert wird. Deshalb besteht ein besonderes Schutzbedürfnis gegen Mißbrauch.