

BESCHLUSSEMPFEHLUNG UND BERICHT

des Innenausschusses (2. Ausschuss)

zu dem Gesetzentwurf der Landesregierung
- Drucksache 3/2219 -

Entwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften

A. Problem

Die Richtlinie 95/46/EG des Europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr gibt den Mitgliedstaaten auf, ihre datenschutzrechtlichen Vorschriften innerhalb von drei Jahren an die Richtlinie anzupassen. Im Interesse der Einheitlichkeit des deutschen Datenschutzrechts war zunächst die Novellierung des Bundesdatenschutzgesetzes abzuwarten, die mit Verabschiedung des Regierungsentwurfs durch das Bundeskabinett am 14. Juni 2000 eingeleitet wurde.

Darüber hinaus ist seit Jahren umstritten, ob Notare der datenschutzrechtlichen Kontrolle durch den Landesbeauftragten für den Datenschutz unterliegen.

B. Lösung

Die Begrifflichkeiten werden an die der EG-Richtlinie angeglichen und die Rechte des Betroffenen verbessert. Die Institution des behördlichen Datenschutzbeauftragten wird geschaffen und eine Vorabkontrolle für Datenverarbeitungsverfahren eingeführt. Regelungen zur Verarbeitung besonderer Kategorien von Daten werden getroffen und die Datenübermittlungen an Drittstaaten wird normiert.

Die Gelegenheit der Novellierung wird ergriffen, um das Landesdatenschutzgesetz den neuen Gefahren und gewandelten Anforderungen moderner Datenverarbeitungstechniken anzupassen. Dabei werden aktualisierte Maßnahmen zur Datensicherheit festgelegt, Regelungen für mobile Datenverarbeitungssysteme, für Verfahren der Videoüberwachung und Videoaufzeichnung und für Fernmess- und Fernwirkdienste geschaffen und ein Datenschutzaudit normiert.

Schließlich bringt der Entwurf bereichsspezifische Datenschutzvorschriften mit dem neuen Landesdatenschutzgesetz in Übereinstimmung, soweit erforderlich und im Rahmen einer zügigen Gesetzesnovellierung möglich.

Die vom Innenausschuss vorgesehenen Änderungen des Gesetzentwurfes tragen der Übernahme der EG-Datenschutz-Richtlinie durch die EWR-Vertragstaaten Rechnung, passen das Sicherheits- und Ordnungsgesetz an die neuen Datenschutzbestimmungen an und korrigieren redaktionelle Unzulänglichkeiten.

Durch eine vom Ausschuss vorgesehene EntschlieÙung wird des Weiteren die Rechtsauffassung zum Ausdruck gebracht, dass auch Notare als Träger eines öffentlichen Amtes der datenschutzrechtlichen Kontrolle durch den Landesbeauftragten für den Datenschutz unterliegen. Zugleich wird die Annahme festgehalten, dass die Landesregierung prüfe, die Datenschutzkontrolle im öffentlichen und privaten Bereich institutionell zu vereinheitlichen.

Einvernehmen im Ausschuss

C. Alternativen

Keine.

D. Kosten

Die Neueinrichtung von behördlichen Datenschutzbeauftragten kann Kosten verursachen, die vor allem bei der erforderlichen datenschutzrechtlichen Bestandsaufnahme entstehen. Nach Abschluss der Einführungsphase und insbesondere dann, wenn von der Möglichkeit Gebrauch gemacht wird, die gleiche Person zum Datenschutzbeauftragten mehrerer Stellen zu bestimmen, ist dagegen von geringerem Aufwand auszugehen.

Beschlussempfehlung

Der Landtag möge beschließen,

1. den Gesetzentwurf der Landesregierung auf Drucksache 3/2219 in der aus der nachfolgenden Zusammenstellung ersichtlichen Fassung anzunehmen.
2. der folgenden EntschlieÙung zuzustimmen:

„Hinsichtlich der Regelung in § 30 geht der Landtag davon aus, dass Notare als unabhängige Träger eines öffentlichen Amtes der Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz unterliegen.

Der Landtag geht davon aus, dass die Landesregierung prüft, die Datenschutzkontrolle im öffentlichen und privaten Bereich institutionell einheitlich zu regeln.“

Schwerin, den 6. März 2002

Der Innenausschuss

Siegfried Friese

Vorsitzender und Berichterstatter

Zusammenstellung

des Entwurfs eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften mit den Beschlüssen des Innenausschusses (2. Ausschuss) ^{*)}

Entwurf	Beschlüsse des 2. Ausschusses
Entwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften	Entwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften
Der Landtag hat das folgende Gesetz beschlossen:	Der Landtag hat das folgende Gesetz beschlossen:
Artikel 1 Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz - DSG M-V)	Artikel 1 Gesetz zum Schutz des Bürgers bei der Verarbeitung seiner Daten (Landesdatenschutzgesetz - DSG M-V)
Inhaltsübersicht	
Abschnitt 1 ALLGEMEINE VORSCHRIFTEN	Abschnitt 1 unverändert
§ 1 Zweck	
§ 2 Anwendungsbereich	
§ 3 Begriffsbestimmungen	
§ 4 Verarbeitung von personenbezogenen Daten im Auftrag	
§ 5 Datenvermeidung, Datenschutzaudit, Systemdatenschutz	
§ 6 Datengeheimnis	

^{*)} Die vom Innenausschuss gegenüber

- dem Text des Gesetzentwurfes der Landesregierung beschlossenen Änderungen und Streichungen sind in der linken Spalte durch Unterstreichung gekennzeichnet, während die jeweilige Neufassung des Textes in der rechten Spalte durch Fettdruck hervorgehoben wird.
- den Überschriften des Gesetzentwurfes der Landesregierung erfolgten Änderungen sind in der rechten Spalte durch Unterstreichung gekennzeichnet.

Entwurf**Abschnitt 2****VERARBEITUNG VON
PERSONENBEZOGENEN DATEN**

- § 7 Grundsatz
- § 8 Einwilligung
- § 9 Erheben
- § 10 Nutzen
- § 11 Speichern, Verändern
- § 12 Automatisierte Einzelentscheidung
- § 13 Berichten, Sperren und Löschen
- § 14 Übermittlung an Stellen innerhalb des öffentlichen Bereichs
- § 15 Übermittlung an inländische nicht-öffentliche Stellen
- § 16 Übermittlung an europäische nicht-öffentliche Stellen und Drittstaaten
- § 17 Verbund- und Abrufverfahren
- § 18 Verfahrensverzeichnis
- § 19 Freigabe, Vorabkontrolle
- § 20 Behördlicher Datenschutzbeauftragter
- § 21 Allgemeine Maßnahmen zur Datensicherheit
- § 22 Besondere Maßnahmen zur Datensicherheit beim Einsatz automatisierter Verfahren
- § 23 Pflicht zur Benachrichtigung Betroffener

Abschnitt 3**RECHTE DES BETROFFENEN**

- § 24 Auskunft, Akteneinsicht
- § 25 Sperrung und Widerspruch durch den Betroffenen
- § 26 Anrufung des Landesbeauftragten für den Datenschutz
- § 27 Schadensersatz
- § 28 Unabdingbarkeit der Rechte Betroffener

**Beschlüsse
des 2. Ausschusses****Abschnitt 2** unverändert**Abschnitt 3** unverändert

Entwurf	Beschlüsse des 2. Ausschusses
Abschnitt 4 DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ	Abschnitt 4 unverändert
§ 29 Berufung und Rechtsstellung	
§ 30 Kontrolle	
§ 31 Unterstützung	
§ 32 Beanstandungen	
§ 33 Weitere Aufgaben und Befugnisse	
Abschnitt 5 BESONDERE REGELUNGEN	Abschnitt 5 unverändert
§ 34 Wissenschaftliche Forschung	
§ 35 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen	
§ 36 Mobile Datenverarbeitungssysteme	
§ 37 Videoüberwachung und -aufzeichnung	
§ 38 Fernmess- und Fernwirkdienste	
§ 39 Öffentliche Auszeichnungen	
Abschnitt 6 PERSONENBEZOGENE DATEN EHEMALIGER EINRICHTUNGEN	Abschnitt 6 unverändert
§ 40 Zuständigkeit für personenbezogene Daten ehemaliger Einrichtungen	
§ 41 Zulässige Nutzung und Zweckbestim- mung der Speicherung personenbezo- gener Daten ehemaliger Einrichtungen	
Abschnitt 7 STRAF-, ÜBERGANGS- UND SCHLUSSVORSCHRIFTEN	Abschnitt 7 unverändert
§ 42 Straftaten	
§ 43 Übergangsvorschrift	
§ 44 Außer-Kraft-Treten	

Entwurf	Beschlüsse des 2. Ausschusses
Abschnitt 1 ALLGEMEINE VORSCHRIFTEN	Abschnitt 1 ALLGEMEINE VORSCHRIFTEN
§ 1 Zweck	§ 1 unverändert
Zweck dieses Gesetzes ist es, das Recht des Einzelnen zu schützen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (Recht auf informationelle Selbstbestimmung).	
§ 2 Anwendungsbereich	§ 2 Anwendungsbereich
(1) Dieses Gesetz gilt für Behörden und öffentlich-rechtliche Einrichtungen und Stellen des Landes, der Gemeinden, der Ämter, der Landkreise sowie für sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts (öffentliche Stellen).	(1) unverändert
(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts, auf die dieses Gesetz nach Satz 1 Anwendung findet, an einer weiteren Vereinigung des privaten Rechts, so findet Satz 1 entsprechende Anwendung. Nehmen nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.	(2) unverändert

Entwurf	Beschlüsse des 2. Ausschusses
<p>(3) Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Verwendung gelöscht werden, sowie für Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen und alsbald vernichtet werden, gelten nur die §§ 6, 21 und 22 sowie die §§ 29 bis 33. Diese Daten sind vor dem Zugriff Unbefugter zu schützen.</p>	(3) unverändert
<p>(4) Soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor. Für die Gerichte sowie für die Behörden der Staatsanwaltschaft gilt dieses Gesetz nur, soweit sie Verwaltungsaufgaben wahrnehmen. Darüber hinaus gelten für die Behörden der Staatsanwaltschaft, soweit sie keine Verwaltungsaufgaben wahrnehmen, die §§ 18, 26, 29 bis 33 und 35 sowie die §§ 39 bis 41; die §§ 24 und 25 finden keine Anwendung.</p>	(4) unverändert
<p>(5) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur die §§ 18, 26, 29 bis 33 sowie die §§ 38 bis 41. Mit Ausnahme der Vorschriften über die Meldepflichten und die Aufsichtsbehörde (§§ <u>32</u> und 38) sind im Übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch Artikel <u>2 Abs. 5</u> des Gesetzes vom <u>17. Dezember 1997</u> (BGBl. I S. <u>3108</u>), einschließlich der §§ 43 und 44 anwendbar.</p>	<p>(5) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur die §§ 18, 26, 29 bis 33 sowie die §§ 38 bis 41. Mit Ausnahme der Vorschriften über die Meldepflichten und die Aufsichtsbehörde (§§ 4 d, 4 e und 38) sind im Übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch Artikel 1 des Gesetzes vom 18. Mai 2001 (BGBl. I S. 904), einschließlich der §§ 43 und 44 anwendbar.</p>
<p>(6) Für Gnadenverfahren findet dieses Gesetz keine Anwendung.</p>	(6) unverändert

Entwurf	Beschlüsse des 2. Ausschusses
§ 3 Begriffsbestimmungen	§ 3 Begriffsbestimmungen
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).	(1) unverändert
(2) Eine Datei ist	(2) unverändert
1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren verarbeitet und ausgewertet werden kann (automatisierte Datei) oder 2. jede sonstige strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist (nicht-automatisierte Datei).	
(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage einschließlich Bild- und Tonträgern, soweit sie nicht eine Datei im Sinne von Absatz 2 ist. Nicht hierunter fallen Vorentwürfe oder Notizen, die nicht Bestandteil eines Vorgangs werden sollen.	(3) unverändert
(4) Datenverarbeitung ist jede Verwendung personenbezogener Daten im Sinne der nachfolgenden Vorschriften. Dabei ist	(4) unverändert
1. Erheben das Beschaffen von Daten, 2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger; dazu zählt auch das Vervielfältigen, 3. Verändern das inhaltliche Umgestalten gespeicherter Daten,	

Entwurf

4. Übermitteln das Bekanntgeben erhobener, gespeicherter oder durch sonstige Verarbeitung gewonnener Daten an Dritte in der Weise, dass die Daten durch die Daten verarbeitende Stelle weitergegeben werden oder dass Dritte von der Daten verarbeitenden Stelle zur Einsicht oder zum Abruf bereit gehaltene Daten einsehen oder abrufen,
5. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten, angenommen in den Fällen, in denen dieses Gesetz die Verarbeitung der Daten zulässt,
6. Löschen das dauerhafte Unkenntlichmachen gespeicherter Daten,
7. Nutzen die inhaltliche Auswertung und Verwendung von Daten,
8. Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr oder nur mit unverhältnismäßig hohem Aufwand einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können,
9. Pseudonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse ohne Anwendung der Zuordnungsfunktion nicht mehr oder nur mit unverhältnismäßig hohem Aufwand einer bestimmten oder bestimmbarer natürlichen Person zugeordnet werden können,
10. Verschlüsseln das Verändern personenbezogener Daten derart, dass ohne Entschlüsselung die Kenntnisnahme des Inhaltes der Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

**Beschlüsse
des 2. Ausschusses**

Entwurf	Beschlüsse des 2. Ausschusses
(5) Daten verarbeitende Stelle ist jede öffentliche Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere in ihrem Auftrag verarbeiten lässt.	(5) unverändert
(6) Dritter ist jede Person oder Stelle außerhalb der Daten verarbeitenden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen oder Stellen, die im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union im Auftrag tätig werden.	(6) Dritter ist jede Person oder Stelle außerhalb der Daten verarbeitenden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen oder Stellen, die im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum im Auftrag tätig werden.
(7) Stellen innerhalb des öffentlichen Bereichs sind öffentliche Stellen nach § 2 Abs. 1 und 2, öffentliche Stellen des Bundes und der anderen Länder nach § 2 des Bundesdatenschutzgesetzes sowie öffentliche Stellen der Europäischen Union <u>und</u> ihrer Mitgliedstaaten.	(7) Stellen innerhalb des öffentlichen Bereichs sind öffentliche Stellen nach § 2 Abs. 1 und 2, öffentliche Stellen des Bundes und der anderen Länder nach § 2 des Bundesdatenschutzgesetzes sowie öffentliche Stellen der Europäischen Union, ihrer Mitgliedstaaten oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum.
(8) Verbundverfahren sind automatisierte Verfahren, die mehreren Daten verarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten ermöglichen.	(8) unverändert
(9) Abrufverfahren sind automatisierte Verfahren, die die Übermittlung personenbezogener Daten durch Abruf ermöglichen.	(9) unverändert

Entwurf	Beschlüsse des 2. Ausschusses
<p>(10) Mobile Datenverarbeitungssysteme sind informationstechnische Systeme, die zum Einsatz in automatisierten Verfahren bestimmt sind, an die Betroffenen ausgegeben werden und über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle personenbezogene Daten automatisiert austauschen können.</p>	<p>(10) unverändert</p>
<p>§ 4 Verarbeitung von personenbezogenen Daten im Auftrag</p>	<p>§ 4 unverändert</p>
<p>(1) Werden personenbezogene Daten durch andere Personen oder Stellen im Auftrag einer öffentlichen Stelle verarbeitet, so bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 24, 25 und 27 genannten Rechte sind ihm gegenüber geltend zu machen. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die Gewährleistung der nach den §§ 21 und 22 notwendigen technisch-organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Art und der Umfang der Verarbeitung von personenbezogenen Daten sowie erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.</p>	
<p>(2) Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder eine andere Vorschrift über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.</p>	

Entwurf

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, sicherzustellen, dass der Auftragnehmer die Vorschriften dieses Gesetzes befolgt und sich der Kontrolle des Landesbeauftragten für den Datenschutz nach Maßgabe der §§ 30 und 31 unterwirft. Der Auftraggeber hat den Landesbeauftragten für den Datenschutz über die Beauftragung zu informieren.

(4) Bei der Erbringung von Wartungs-, Fernwartungs- und anderen Hilfstätigkeiten durch Stellen oder Personen außerhalb der Daten verarbeitenden Stelle gelten die Absätze 1 bis 3 entsprechend, soweit die Tätigkeiten mit der Verarbeitung von personenbezogenen Daten verbunden sind. Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass der Auftragnehmer personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidlich ist.

§ 5 Datenvermeidung, Datenschutzaudit, Systemdatenschutz

(1) Die Gestaltung von Verfahren und die Auswahl von informationstechnischen Produkten zum Einsatz in automatisierten Verfahren hat sich am Grundsatz größtmöglicher Datenvermeidung zu orientieren. Personenbezogene Daten sind zu anonymisieren und hilfsweise zu pseudonymisieren, sobald dies möglich ist und soweit der erforderliche Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht.

**Beschlüsse
des 2. Ausschusses**

§ 5 unverändert

Entwurf

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

(3) Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

§ 6 Datengeheimnis

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

**Beschlüsse
des 2. Ausschusses****§ 6 unverändert**

Entwurf	Beschlüsse des 2. Ausschusses
Abschnitt 2 VERARBEITUNG VON PERSONENBEZOGENEN DATEN	Abschnitt 2 VERARBEITUNG VON PERSONENBEZOGENEN DATEN
§ 7 Grundsatz	§ 7 unverändert
(1) Die Verarbeitung von personenbezogenen Daten ist nur zulässig, soweit	
<ol style="list-style-type: none">1. die Vorschriften dieses Gesetzes sie zulassen,2. eine andere Rechtsvorschrift sie erlaubt oder zwingend voraussetzt oder3. der Betroffene eingewilligt hat.	
(2) Die Verarbeitung personenbezogener Daten,	
<ol style="list-style-type: none">1. aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen oder2. die die Gesundheit oder das Sexualleben betreffen,	
ist nur zulässig, wenn eine Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt, sie ausdrücklich erlaubt.	
(3) Abweichend von Absatz 2 ist die Verarbeitung der dort genannten Daten zulässig	
<ol style="list-style-type: none">1. wenn der Betroffene ausdrücklich eingewilligt hat,2. auf der Grundlage der §§ 34, 35 und 39,	

Entwurf

3. wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,
4. wenn sie ausschließlich im Interesse des Betroffenen liegt und der Landesbeauftragte für den Datenschutz zuvor gehört worden ist. In Eilfällen kann die Anhörung nachgeholt werden.

(4) Privatrechtliche Stellen oder Vereinigungen, die nach § 2 Abs. 2 als öffentliche Stellen gelten, dürfen personenbezogene Daten, die Straftaten betreffen, nur unter behördlicher Aufsicht oder aufgrund einer Rechtsvorschrift verarbeiten, die den Zweck der Verarbeitung bestimmt.

(5) Sind die zur Aufgabenerfüllung notwendigen Daten in Akten oder in nicht-automatisierten Dateien mit anderen oder mit gesperrten Daten derart verbunden, dass eine Trennung der Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, so sind die Kenntnisnahme, die Mitspeicherung und Mitveränderung sowie die Übermittlung auch der nicht benötigten Daten zulässig, soweit nicht schutzwürdige Belange des Betroffenen überwiegen. Diese Daten dürfen nicht weiter verarbeitet werden. Darauf ist der Empfänger im Falle der Übermittlung in geeigneter Weise hinzuweisen.

**Beschlüsse
des 2. Ausschusses**

Entwurf**§ 8 Einwilligung**

(1) Die Einwilligung des Betroffenen bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Sie muss sich im Falle einer Datenverarbeitung nach § 7 Abs. 2 ausdrücklich auch auf die dort genannten Daten beziehen. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich eingeholt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild des Schriftstücks hervorzuheben. Der Betroffene ist in geeigneter Weise über die Bedeutung und Tragweite der Einwilligung, insbesondere über die Art und den Umfang der Verarbeitung sowie über Empfänger beabsichtigter Übermittlungen von Daten, aufzuklären. Die Anschrift der Daten verarbeitenden Stelle ist ihm mitzuteilen. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.

(2) Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, dass

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

**Beschlüsse
des 2. Ausschusses****§ 8 unverändert**

Entwurf	Beschlüsse des 2. Ausschusses
§ 9 Erheben	§ 9 Erheben
<p>(1) Das Erheben personenbezogener Daten ist zulässig, wenn deren Kenntnis zur rechtmäßigen Erfüllung einer in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist, der Zweck der Erhebung hinreichend bestimmt ist und die Daten ohne Verstoß gegen Rechtsvorschriften offenbart werden können.</p>	<p>(1) unverändert</p>
<p>(2) Personenbezogene Daten sind beim Betroffenen und mit seiner Kenntnis zu erheben, es sei denn, dass eine Rechtsvorschrift eine andere Art der Erhebung erlaubt oder zwingend voraussetzt oder dass der Betroffene in eine andere Art der Erhebung eingewilligt hat.</p>	<p>(2) unverändert</p>
<p>(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist er von der Daten verarbeitenden Stelle in geeigneter Weise über den Zweck der Erhebung, die Art und den Umfang der Verarbeitung <u>und Nutzung</u>, über Empfänger beabsichtigter Übermittlungen der Daten sowie über das Bestehen von Auskunfts- oder Berichtigungsansprüchen aufzuklären. Die Anschrift der Daten verarbeitenden Stelle ist ihm mitzuteilen. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Er ist über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.</p>	<p>(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist er von der Daten verarbeitenden Stelle in geeigneter Weise über den Zweck der Erhebung, die Art und den Umfang der Verarbeitung, über Empfänger beabsichtigter Übermittlungen der Daten sowie über das Bestehen von Auskunfts- oder Berichtigungsansprüchen aufzuklären. Die Anschrift der Daten verarbeitenden Stelle ist ihm mitzuteilen. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Er ist über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.</p>

Entwurf

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

§ 10 Nutzen

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

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

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

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,

**Beschlüsse
des 2. Ausschusses**

(4) unverändert

§ 10 unverändert

Entwurf

4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,
6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
7. es zur Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Absatz 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes in der Fassung der Bekanntmachung vom 11. Dezember 1974 (BGBl. I S. 3427), zuletzt geändert nach Maßgabe des Artikels 8 durch Artikel 3 des Gesetzes vom 26. Januar 1998 (BGBl. I S. 160), oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder
9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

**Beschlüsse
des 2. Ausschusses**

Entwurf

Der andere Zweck muss hinreichend bestimmt sein. Besondere Amts- oder Berufsheimnisse bleiben unberührt. Für Daten im Sinne von § 7 Abs. 2 findet Satz 1 Nr. 3 keine Anwendung.

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

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

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der Daten verarbeitenden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür genutzt werden dürften, wenn sie nicht gesperrt wären.

**Beschlüsse
des 2. Ausschusses**

Entwurf

(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 genutzt werden, es sei denn, der Betroffene willigt ein.

§ 11 Speichern, Verändern

(1) Das Speichern und Verändern personenbezogener Daten ist zulässig, wenn es zur Erfüllung einer in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist.

(2) Personenbezogene Daten dürfen nur zu Zwecken ihrer zulässigen Nutzung nach § 10 und in dem dafür notwendigen Umfang gespeichert oder verändert werden.

§ 12 Automatisierte Einzelentscheidung

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf der automatisierten Verarbeitung personenbezogener Daten zum Zwecke der Bewertung einzelner Persönlichkeitsmerkmale beruhen, sondern sind in jedem Einzelfall durch eine natürliche Person zu überprüfen. Satz 1 gilt nicht, wenn

1. ein Gesetz dies vorsieht oder
2. der Betroffene vor der Entscheidung die Möglichkeit erhält, seine besonderen persönlichen Interessen geltend zu machen.

**Beschlüsse
des 2. Ausschusses**

§ 11 unverändert

§ 12 unverändert

Entwurf**§ 13 Berichtigen, Sperren und Löschen**

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

(2) Personenbezogene Daten sind zu löschen, wenn

1. sie unrichtig sind und die Daten verarbeitende Stelle keine Kenntnis der richtigen Daten erlangen kann,
2. ihre Erhebung unzulässig war,
3. ihre Speicherung unzulässig ist oder
4. ihre Speicherung zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe nicht mehr erforderlich ist.

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

1. einer Löschung nach Absatz 2 Nr. 4 Rechtsvorschriften entgegenstehen,
2. Grund zur Annahme besteht, dass durch die Berichtigung oder Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden,
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder
4. es der Betroffene nach § 25 verlangt.

**Beschlüsse
des 2. Ausschusses**

§ 13 unverändert

Entwurf

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

(5) Gesperrte Daten sind gesondert zu speichern. Ist dies nicht möglich, so sind die Daten mit einem entsprechenden Vermerk zu versehen. Gesperrte Daten dürfen über ihre Speicherung hinaus, außer zu Zwecken ihrer zulässigen Nutzung und in den Fällen des § 7 Abs. 5 nicht mehr verarbeitet werden. Gesperrte Daten dürfen vor Ablauf ihrer Sperrfrist nur verändert oder gelöscht werden, wenn ein Grund für eine Berichtigung gegeben ist; in diesem Falle ist der ursprüngliche Zustand zu dokumentieren.

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

(7) Werden durch eine Daten verarbeitende Stelle unrichtige, unzulässig erhobene oder unzulässig gespeicherte Daten berichtet, gesperrt oder gelöscht, so benachrichtigt diese andere Stellen, die diese Daten ebenfalls verarbeiten, insbesondere die Empfänger von Übermittlungen. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßig hohen Aufwand erfordern würde und kein Grund zur Annahme besteht, dass dadurch schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

**Beschlüsse
des 2. Ausschusses**

Entwurf**§ 14 Übermittlung an Stellen innerhalb
des öffentlichen Bereichs**

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

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

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

**Beschlüsse
des 2. Ausschusses**

§ 14 unverändert

Entwurf**§ 15 Übermittlung an inländische
nicht-öffentliche Stellen**

(1) Die Übermittlung personenbezogener Daten an inländische Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn dies zur Erfüllung einer in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe erforderlich ist oder wenn die Nutzung der Daten zur Erfüllung einer in der Zuständigkeit des Empfängers liegenden Aufgabe erforderlich und nach § 10 zulässig ist. Darüber hinaus ist sie zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. In diesem Falle unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung. Dies gilt nicht, wenn er davon auf andere Weise Kenntnis erlangt oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

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

**Beschlüsse
des 2. Ausschusses****§ 15 unverändert**

Entwurf**§ 16 Übermittlung an europäische nicht-öffentliche Stellen und Drittstaaten**

(1) Für die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen in Mitgliedstaaten der Europäischen Union gilt § 15 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Verordnungen. Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen wird.

(2) Für die Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union sowie an sonstige über- und zwischenstaatliche Stellen gilt § 15 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Verordnungen, wenn im Empfängerland ein angemessener Datenschutz gewährleistet ist. Dies gilt nicht, soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen wird.

(3) Sofern im Empfängerland kein angemessener Datenschutz gewährleistet ist, ist eine Übermittlung zulässig, wenn

1. der Betroffene seine Einwilligung erteilt hat,
2. die Übermittlung zur Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
3. die Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist,

**Beschlüsse
des 2. Ausschusses****§ 16 Übermittlung an europäische nicht-öffentliche Stellen und Drittstaaten**

(1) Für die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen in Mitgliedstaaten der Europäischen Union **oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum** gilt § 15 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Verordnungen. Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen wird.

(2) Für die Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union **und der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum** sowie an sonstige über- und zwischenstaatliche Stellen gilt § 15 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Verordnungen, wenn im Empfängerland ein angemessener Datenschutz gewährleistet ist. Dies gilt nicht, soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen wird.

(3) unverändert

Entwurf

4. die Übermittlung aus einem für die Information der Öffentlichkeit bestimmten Register erfolgt und die Voraussetzungen für die Einsichtnahme im Einzelfall vorliegen oder
5. die empfangende Stelle ausreichende Garantien für den Schutz der Grundrechte bietet und die für die übermittelnde Stelle zuständige Rechtsaufsichtsbehörde die Übermittlung genehmigt.

(4) Die Angemessenheit des Datenschutzes im Empfängerland wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen; insbesondere werden die Art der Daten, die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die beim Empfängerland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Landesregeln und Sicherheitsmaßnahmen berücksichtigt.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Die empfangende Stelle ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet werden dürfen, zu dessen Erfüllung sie ihm übermittelt werden.

(6) Die übermittelnde Stelle teilt dem Landesbeauftragten für den Datenschutz ihre Feststellung über die Angemessenheit des Datenschutzes im Empfängerland mit. Ferner teilt sie ihm die nach Absatz 3 Nr. 5 erteilten Genehmigungen der Rechtsaufsichtsbehörde mit. Der Landesbeauftragte für den Datenschutz teilt die nach Absatz 3 Nr. 5 erteilten Genehmigungen der Rechtsaufsichtsbehörde dem Bund mit.

**Beschlüsse
des 2. Ausschusses**

(4) unverändert

(5) unverändert

Entwurf**§ 17 Verbund- und Abrufverfahren**

(1) Ein Verbund- oder Abrufverfahren darf nur eingeführt werden, wenn dies unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die gesetzlichen Anforderungen an die Zulässigkeit der Datenverarbeitung bleiben unberührt. Der Landesbeauftragte für den Datenschutz ist vorab über die Einrichtung des Verfahrens zu informieren.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Verfahrens kontrolliert werden kann. Hierzu ist das Verfahrensverzeichnis nach § 18 jeder beteiligten Stelle um die Feststellung zu ergänzen, für welchen Bereich der Datenverarbeitung jede der beteiligten Stellen verantwortlich ist.

(3) Die Betroffenen können ihre Rechte mit Ausnahme der Rechte nach § 26 gegenüber jeder der beteiligten Stellen geltend machen, unabhängig davon, welche Stelle für die Datenverarbeitung verantwortlich ist. Die beteiligten Stellen leiten die Anliegen der Betroffenen an die nach Absatz 2 zuständige Stelle weiter.

(4) Die Absätze 1 bis 3 gelten entsprechend, wenn innerhalb einer verarbeitenden Stelle ein Verbund- oder Abrufverfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

(5) Nicht-öffentliche Stellen können sich an Verbund- und Abrufverfahren beteiligen, wenn eine Rechtsvorschrift dies zulässt und sie sich insoweit den Vorschriften dieses Gesetzes unterwerfen.

**Beschlüsse
des 2. Ausschusses**

§ 17 unverändert

Entwurf**§ 18 Verfahrensverzeichnis**

(1) Die Daten verarbeitende Stelle ist verpflichtet, in einer Beschreibung für jedes von ihr eingesetzte Verfahren festzulegen und dem behördlichen Datenschutzbeauftragten zur Führung des Verzeichnisses zu übermitteln:

1. die Bezeichnung des Verfahrens und der verarbeitenden Stelle,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Art der gespeicherten Daten,
4. den Kreis der Betroffenen,
5. den Kreis der Empfänger, denen die Daten mitgeteilt werden,
6. geplante Datenübermittlungen in Drittländer,
7. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach den §§ 21 und 22.

(2) Das Verfahrensverzeichnis ist laufend auf dem neuesten Stand zu halten. Es ist dem Landesbeauftragten für den Datenschutz auf Anforderung zu übermitteln.

(3) Die Absätze 1 und 2 gelten nicht für nicht-automatisierte Verfahren, bei denen keine personenbezogene Daten an Dritte übermittelt werden.

§ 19 Freigabe, Vorabkontrolle

(1) Die Einrichtung oder die wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten bedarf der Freigabe durch den Leiter der Daten verarbeitenden Stelle oder einen dafür beauftragten Vertreter. Die Freigabe hat schriftlich zu erfolgen.

**Beschlüsse
des 2. Ausschusses****§ 18 unverändert****§ 19 unverändert**

Entwurf

(2) Vor der Einrichtung oder wesentliche Änderung eines Verfahrens nach Absatz 1,

1. auf das § 17 Abs. 1 Anwendung findet oder
2. in dem Daten im Sinne von § 7 Abs. 2 verarbeitet werden,

ist dem behördlichen Datenschutzbeauftragten Gelegenheit zur Prüfung innerhalb einer angemessenen Frist zu geben, ob die Datenverarbeitung zulässig und die vorgesehenen Maßnahmen nach den §§ 21 und 22 ausreichend sind. Satz 1 gilt nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

(3) Die Landesregierung kann Anforderungen an die Freigabe nach Absatz 1, an das Sicherheitskonzept nach § 22 Abs. 5 sowie weitere Einzelheiten einer ordnungsgemäßen Datenverarbeitung der öffentlichen Stellen durch Rechtsverordnung regeln. Der Landesbeauftragte für den Datenschutz ist anzuhören.

**Beschlüsse
des 2. Ausschusses**

Entwurf**§ 20 Behördlicher Datenschutzbeauftragter**

(1) Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Der behördliche Datenschutzbeauftragte soll Beschäftigter der Daten verarbeitenden Stelle sein; soweit dadurch die Erfüllung seiner Aufgaben nicht beeinträchtigt wird, können mehrere Daten verarbeitende Stellen denselben behördlichen Datenschutzbeauftragten bestellen. Bestellt werden darf nur, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird und die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit besitzt. Der behördliche Datenschutzbeauftragte ist bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes unabhängig und weisungsfrei. Er ist dem Leiter der öffentlichen Stelle unmittelbar unterstellt, kann sich direkt an ihn wenden und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Beschäftigten der Daten verarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden. Auf den behördlichen Datenschutzbeauftragten findet § 29 Abs. 8 entsprechende Anwendung.

(2) Die Bestellung zum behördlichen Datenschutzbeauftragten kann befristet werden. Sie kann schriftlich widerrufen werden, wenn ein Interessenkonflikt mit seinen anderen dienstlichen Aufgaben eintritt oder sonst ein wichtiger Grund in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches vorliegt. Vor der Entscheidung über den Widerruf ist der behördliche Datenschutzbeauftragte zu hören.

**Beschlüsse
des 2. Ausschusses****§ 20 Behördlicher Datenschutzbeauftragter**

(1) Die Daten verarbeitende Stelle hat schriftlich einen behördlichen Datenschutzbeauftragten sowie einen Vertreter zu bestellen. Der behördliche Datenschutzbeauftragte soll Beschäftigter der Daten verarbeitenden Stelle sein; soweit dadurch die Erfüllung seiner Aufgaben nicht beeinträchtigt wird, können mehrere Daten verarbeitende Stellen denselben behördlichen Datenschutzbeauftragten bestellen. Bestellt werden darf nur, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird und die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit besitzt. Der behördliche Datenschutzbeauftragte ist bei der Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes unabhängig und weisungsfrei. Er ist dem Leiter der öffentlichen Stelle unmittelbar unterstellt, kann sich direkt an ihn wenden und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Beschäftigten der Daten verarbeitenden Stelle können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an ihn wenden.

(2) unverändert

Entwurf**Beschlüsse
des 2. Ausschusses**

(3) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu überwachen und Hinweise zur Umsetzung zu geben. Er kann Auskünfte verlangen und Einsicht in Akten und Dateien nehmen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Berufs- und Amtsgeheimnisse können ihm nicht entgegengehalten werden. Zu seiner Unterstützung kann er sich jederzeit an den Landesbeauftragten für den Datenschutz wenden. Zu seinen Aufgaben gehört es insbesondere,

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,
3. die Daten verarbeitende Stelle bei der Umsetzung der nach den §§ 18, 21 und 22 erforderlichen Maßnahmen zu unterstützen,
4. das Verzeichnis nach § 18 zu führen und
5. die Vorabkontrolle nach § 19 durchzuführen.

(4) Das Verzeichnis nach § 18 Abs. 1 kann von jedermann eingesehen werden. Dies gilt nicht für die Angaben nach § 18 Abs. 1 Nr. 7 und die Verfahren, die nach § 24 Abs. 4 Nr. 2 und 3 nicht der Auskunftspflicht unterliegen.

(3) unverändert

(4) unverändert

Entwurf**§ 21 Allgemeine Maßnahmen zur
Datensicherheit**

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und nach der Schutzbedürftigkeit der zu verarbeitenden Daten erforderlich und angemessen sind.

(2) Dabei ist insbesondere zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität der Daten),
5. unter Beteiligung der Personal- oder Arbeitnehmersvertretung von der Daten verarbeitenden Stelle ein Protokollierungsverfahren festgelegt wird, das die Feststellung erlaubt, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit) und
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig und in zumutbarer Zeit nachvollzogen werden können (Transparenz).

**Beschlüsse
des 2. Ausschusses**

§ 21 unverändert

Entwurf**§ 22 Besondere Maßnahmen zur
Datensicherheit beim Einsatz
automatisierter Verfahren**

(1) Automatisierte Verfahren sind so zu gestalten, dass eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung 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 verarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln.

(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 Protokollbestände 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) In einem Sicherheitskonzept ist für jedes automatisierte Verfahren festzulegen, in welcher Form die Anforderungen des § 21 und der Absätze 1 bis 4 umzusetzen sind.

**Beschlüsse
des 2. Ausschusses**

§ 22 unverändert

Entwurf	Beschlüsse des 2. Ausschusses
<p data-bbox="268 324 689 385">§ 23 Pflicht zur Benachrichtigung Betroffener</p> <p data-bbox="181 427 778 719">Hat eine Daten verarbeitende Stelle Grund zur Annahme oder Kenntnis, dass unrichtige, unzulässig erhobene oder unzulässig gespeicherte personenbezogene Daten in der Weise genutzt wurden, dass dem Betroffenen daraus ein Nachteil entstanden ist oder zu entstehen droht, so hat sie diesen unverzüglich zu benachrichtigen.</p>	<p data-bbox="970 324 1184 362">§ 23 unverändert</p>
<p data-bbox="181 795 566 855">Abschnitt 3 RECHTE DES BETROFFENEN</p>	<p data-bbox="785 795 1168 855">Abschnitt 3 RECHTE DES BETROFFENEN</p>
<p data-bbox="300 896 662 929">§ 24 Auskunft, Akteneinsicht</p>	<p data-bbox="896 896 1259 929">§ 24 Auskunft, Akteneinsicht</p>
<p data-bbox="181 967 778 1034">(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über</p> <ol data-bbox="181 1079 778 1444" style="list-style-type: none">1. die zu seiner Person gespeicherten Daten,2. die verfügbaren Informationen über die Herkunft der Daten und die Empfänger, an die die Daten übermittelt werden,3. den Zweck und die Rechtsgrundlage der Verarbeitung,4. die Funktionsweise des Verarbeitungsverfahrens im Falle einer zulässigen automatisierten Einzelentscheidung nach § 12.	<p data-bbox="785 967 986 1001">(1) unverändert</p>
<p data-bbox="181 1489 778 1852">In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, soll der Betroffene Angaben machen, die das Auffinden der Daten ermöglichen. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.</p>	

Entwurf	Beschlüsse des 2. Ausschusses
(2) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.	(2) unverändert
<u>(3) Die Auskunftserteilung unterbleibt, soweit</u>	(3) entfällt
<ol style="list-style-type: none"> <li data-bbox="178 808 778 958">1. <u>die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben gefährden würde,</u> <li data-bbox="178 958 778 1108">2. <u>die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder</u> <li data-bbox="178 1108 778 1328">3. <u>die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder dem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen</u> 	
<u>und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.</u>	
<u>(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.</u>	(4) entfällt hier, siehe Absatz 5

Entwurf

(5) 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 Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(6) Die Auskunftserteilung oder die Gewährung von Einsicht unterbleibt, soweit eine Prüfung ergibt, dass

1. dadurch die Erfüllung der Aufgaben der Daten verarbeitenden 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 geheim gehalten werden müssen.

**Beschlüsse
Des 2. Ausschusses**

(3) unverändert

(4) unverändert

(5) Die Ablehnung der Auskunftserteilung **und die Versagung der Einsichtnahme bedürfen** keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung **oder der Versagung der Akteneinsicht** verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.

Entwurf	Beschlüsse des 2. Ausschusses
<p>(7) Wird dem Betroffenen keine Auskunft oder Einsicht gewährt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Landesbeauftragten für den Datenschutz an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der Daten verarbeitenden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zugestimmt hat.</p>	<p>(6) unverändert</p>
<p>(8) Auskunft und Akteneinsicht sind unentgeltlich.</p>	<p>(7) unverändert</p>
<p>§ 25 Sperrung und Widerspruch durch den Betroffenen</p>	<p>§ 25 unverändert</p>
<p>(1) Der Betroffene hat das Recht, personenbezogene Daten sperren zu lassen, soweit er deren Richtigkeit bestreitet und sich weder die Richtigkeit noch die Unrichtigkeit nachweisen lässt.</p>	
<p>(2) Der Betroffene hat das Recht, bis zur Klärung von Schadensersatzansprüchen unrichtige, unzulässig erhobene oder unzulässig gespeicherte Daten zu seiner Person, die bereits genutzt wurden, auf Antrag bei der Daten verarbeitenden Stelle sperren zu lassen. Die Sperrung wird nach Ablauf von sechs Monaten vom Zeitpunkt des Sperrantrags an unwirksam, wenn durch den Betroffenen innerhalb dieses Zeitraums kein Schadensersatzanspruch gerichtlich geltend gemacht wurde.</p>	

Entwurf

(3) Der Betroffene kann gegenüber der Daten verarbeitenden Stelle der Verarbeitung seiner Daten schriftlich widersprechen, wenn er geltend macht, dass die Verarbeitung seine besonderen persönlichen Interessen beeinträchtigt. In diesem Fall ist die Datenverarbeitung nur zulässig, wenn sie überwiegend im öffentlichen Interesse liegt. Das Prüfungsergebnis mit Begründung ist dem Betroffenen schriftlich mitzuteilen. Die Sätze 1 bis 3 finden keine Anwendung auf Verfahren, die der Gefahrenabwehr, der Strafverfolgung oder der Steuerfahndung dienen.

(4) Der Betroffene ist von der Daten verarbeitenden Stelle über ihre Absicht der Weitergabe seiner Daten zum Zwecke der Direktwerbung rechtzeitig zu informieren. Er ist ausdrücklich auf sein Recht hinzuweisen, einer solchen Weitergabe kostenfrei zu widersprechen.

§ 26 Anrufung des Landesbeauftragten für den Datenschutz

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

**Beschlüsse
des 2. Ausschusses****§ 26 unverändert**

Entwurf**§ 27 Schadensersatz**

(1) Verletzt eine Daten verarbeitende Stelle durch eine unzulässige oder unrichtige automatisierte Verarbeitung personenbezogener Daten die Rechte eines Betroffenen, so ist sie ihm unabhängig von einem Verschulden zum Ersatz des daraus entstehenden Schadens verpflichtet.

(2) Die Schadensersatzpflicht der Daten verarbeitenden Stelle tritt auch bei nicht-automatisierter Verarbeitung ein, es sei denn, die Daten verarbeitende Stelle weist nach, dass sie den Schaden nicht zu vertreten hat.

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

(4) Die Ansprüche nach den Absätzen 1 bis 3 sind insgesamt bis zu einer Höhe von 125 000 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 125 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(5) Sind an einem Verfahren mehrere Daten verarbeitende Stellen beteiligt und ist der Geschädigte nicht in der Lage, die verursachende Stelle festzustellen, so haftet jede dieser Stellen.

(6) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

**Beschlüsse
des 2. Ausschusses****§ 27 unverändert**

Entwurf	Beschlüsse des 2. Ausschusses
<p>(7) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.</p> <p>(8) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verantwortlich ist, bleiben unberührt.</p> <p>(9) Der Rechtsweg vor den ordentlichen Gerichten steht offen.</p>	
<p>§ 28 Unabdingbarkeit der Rechte Betroffener</p>	<p>§ 28 unverändert</p>
<p>Die Rechte nach den §§ 24 bis 27 können auch durch die Einwilligung des Betroffenen nicht ausgeschlossen oder beschränkt werden.</p>	
<p>Abschnitt 4 DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ</p>	<p>Abschnitt 4 DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ</p>
<p>§ 29 Berufung und Rechtsstellung</p>	<p>§ 29 unverändert</p>
<p>(1) Das Amt des Landesbeauftragten für den Datenschutz wird beim Präsidenten des Landtags eingerichtet.</p> <p>(2) Der Landtag wählt ohne Aussprache den Landesbeauftragten für den Datenschutz mit mehr als der Hälfte seiner Mitglieder für die Dauer von sechs Jahren. Die Wiederwahl ist nur einmal zulässig. Vorschlagsberechtigt sind die Fraktionen des Landtags. Kommt vor Ablauf der Amtszeit eine Neuwahl nicht zustande, führt der Landesbeauftragte für den Datenschutz das Amt bis zur Neuwahl weiter.</p>	

Entwurf

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

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

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

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

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

**Beschlüsse
des 2. Ausschusses**

Entwurf

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

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

§ 30 Kontrolle

(1) Der Landesbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen. Diese Kontrolle erstreckt sich auch auf die datenschutzrechtliche Aufsicht der zuständigen Behörden gegenüber den nicht-öffentlichen Stellen. Er kontrolliert die Einhaltung der Datenschutzvorschriften auch bei Stellen, die sich und soweit sie sich seiner Kontrolle unterworfen haben.

(2) Der Landesbeauftragte für den Datenschutz teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung der festgestellten Mängel bei der Verarbeitung von personenbezogenen Daten, verbinden. § 32 bleibt unberührt.

**Beschlüsse
des 2. Ausschusses****§ 30 unverändert**

Entwurf**§ 31 Unterstützung**

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

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen zu gewähren, die im Zusammenhang mit der Datenverarbeitung stehen, namentlich in die gespeicherten Daten sowie in die Datenverarbeitungssysteme und Programme, und
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.

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

§ 32 Beanstandungen

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

1. bei den Behörden des Landes gegenüber der zuständigen obersten Landesbehörde,
2. bei den Gemeinden, Ämtern und Landkreisen gegenüber dem verwaltungsleitenden Organ,

**Beschlüsse
des 2. Ausschusses**

§ 31 unverändert

§ 32 unverändert

Entwurf

3. bei den Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ,
4. bei privatrechtlichen Stellen nach § 2 Abs. 2 gegenüber dem gesetzlichen Vertreter

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

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

(3) Die gemäß Absatz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Landesbeauftragten für den Datenschutz getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 2 und 3 genannten Stellen leiten der zuständigen obersten Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz zu.

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

**Beschlüsse
des 2. Ausschusses**

Entwurf**§ 33 Weitere Aufgaben und Befugnisse**

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

(2) Der Landesbeauftragte für den Datenschutz berät die obersten Landesbehörden sowie die sonstigen öffentlichen Stellen in Fragen des Datenschutzes. Dabei kann er Empfehlungen zur Verbesserung des Datenschutzes geben. Der Landtag und die Landesregierung können den Landesbeauftragten für den Datenschutz mit der Erstellung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen betrauen. Vor dem Erlass oder der Änderung von Rechts- oder Verwaltungsvorschriften, die das Recht auf informationelle Selbstbestimmung berühren, ist der Landesbeauftragte für den Datenschutz zu hören.

**Beschlüsse
des 2. Ausschusses**

§ 33 unverändert

Entwurf

(3) Der Landesbeauftragte für den Datenschutz wirkt auf eine Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den für nicht-öffentliche Stellen nach dem Bundesdatenschutzgesetz zuständigen Aufsichtsbehörden hin. Im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union kann der Landesbeauftragte für den Datenschutz die für die Ausübung der Kontrolle im öffentlichen Bereich zuständigen Stellen um Amtshilfe ersuchen und ist auf Ersuchen selber zur Amtshilfe verpflichtet.

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

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

**Beschlüsse
des 2. Ausschusses**

Entwurf**Abschnitt 5
BESONDERE REGELUNGEN****§ 34 Wissenschaftliche Forschung**

(1) Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken soll in anonymisierter Form erfolgen. Stehen einer Anonymisierung wissenschaftliche Gründe entgegen, können die Daten auch in pseudonymisierter Form verarbeitet werden, wenn der mit der Forschung befasste Personenkreis oder die empfangende Stelle oder Person keinen Zugriff auf die Zuordnungsfunktion hat. Datenerfassung, Anonymisierung und Pseudonymisierung können auch durch die mit der Forschung befassten Personen erfolgen, wenn sie zuvor zur Verschwiegenheit verpflichtet worden sind.

(2) Ist eine Anonymisierung oder Pseudonymisierung nicht möglich, können personenbezogene Daten für ein Forschungsvorhaben verarbeitet werden, wenn

1. der Betroffene eingewilligt hat,
2. dessen schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Nutzung nicht beeinträchtigt werden oder
3. die zuständige oberste Aufsichtsbehörde festgestellt hat, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

**Beschlüsse
des 2. Ausschusses**

Abschnitt 5 unverändert

Entwurf

Sollen personenbezogene Daten übermittelt werden, ist in der Feststellung nach Nr. 3 der Empfänger, die Art der zu übermittelnden personenbezogenen Daten, der Kreis der Betroffenen und der Forschungszweck zu bezeichnen; sie ist dem Landesbeauftragten für den Datenschutz mitzuteilen. Diese Feststellung kann entfallen, wenn eine forschende Person die Anonymisierung innerhalb der Daten verarbeitenden Stelle vornimmt und der behördliche Datenschutzbeauftragte dem Verfahren zustimmt.

Sobald der Forschungszweck dies gestattet, sind die Daten zu anonymisieren, hilfsweise zu pseudonymisieren. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit und solange der Forschungszweck dies erfordert. Sie müssen gelöscht werden, sobald der Forschungszweck dies gestattet.

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

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

**Beschlüsse
des 2. Ausschusses**

Entwurf

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

1. der Betroffene eingewilligt hat oder
2. dieses für die Darstellung von Forschungsergebnissen über die Ereignisse der Zeitgeschichte unerlässlich ist.

(6) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten an ihn nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften des Absatzes 2 Satz 4 bis 7 sowie der Absätze 3 bis 5 einzuhalten und sich der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft.

§ 35 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

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

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

1. der Betroffene eingewilligt hat,
2. eine Rechtsvorschrift dies vorsieht,
3. Art oder Zielsetzung der einem Beschäftigten übertragenen Aufgabe oder der Dienstverkehr es erfordert oder

**Beschlüsse
des 2. Ausschusses**

Entwurf

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

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

(4) Das Erheben medizinischer Daten aufgrund ärztlicher Untersuchungen zum Zwecke der Eingehung eines Dienst- oder Arbeitsverhältnisses ist nur zulässig, soweit dadurch die Eignung des Bewerbers hierfür festgestellt wird und er seine Einwilligung erteilt hat. Das Erheben psychologischer Daten zur Eingehung eines Dienst- oder Arbeitsverhältnisses ist nur zulässig, soweit dies wegen der besonderen Anforderungen an die vorgesehene Tätigkeit erforderlich ist und der Bewerber hierzu seine Einwilligung erteilt hat. Der Dienstherr darf nur das Ergebnis der Untersuchungen anfordern.

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

**Beschlüsse
des 2. Ausschusses**

Entwurf

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

(7) Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 21 und 22 gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

§ 36 Mobile Datenverarbeitungssysteme

(1) Mobile Datenverarbeitungssysteme dürfen nur eingesetzt werden, wenn

1. eine Rechtsvorschrift, eine tarifvertragliche Regelung oder eine Dienstvereinbarung dies zulässt oder
2. der Betroffene eingewilligt hat.

(2) Für den Betroffenen muss jederzeit erkennbar sein,

1. ob Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlasst durchgeführt werden,
2. welche seiner personenbezogenen Daten betroffen sind und
3. welcher Verarbeitungsvorgang im Einzelnen abläuft oder angestoßen wird.

Dem Betroffenen sind die Informationen nach Nummer 2 und 3 auf seinen Wunsch schriftlich mitzuteilen.

**Beschlüsse
des 2. Ausschusses**

Entwurf

(3) Der Betroffene ist bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihm zustehenden Rechte aufzuklären. Sofern zur Wahrnehmung der Informationsrechte besondere Geräte oder Einrichtungen erforderlich sind, hat die ausgebende Stelle dafür zu sorgen, dass diese in angemessenem Umfang unentgeltlich zur Verfügung stehen.

(4) Der Betroffene kann die ihm zustehenden Rechte gegenüber der ausgebenden sowie jeder anderen Stelle geltend machen, die das mobile Datenverarbeitungssystem zur Datenverarbeitung einsetzt. Dies gilt unabhängig davon, welche Stelle im Einzelfall für die jeweilige Datenverarbeitung verantwortlich ist. Die beteiligten Stellen leiten die Anliegen des Betroffenen an die zuständige Stelle weiter.

§ 37 Videoüberwachung und -aufzeichnung

(1) Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten, soweit

1. dies zur Wahrnehmung eines Hausrechts erforderlich ist,
2. schutzwürdige Belange Betroffener nicht überwiegen und
3. die Überwachung durch geeignete Maßnahmen erkennbar gemacht wurde.

**Beschlüsse
des 2. Ausschusses**

Entwurf

(2) Das Bildmaterial darf gespeichert werden, wenn dies zur Abwendung einer konkreten Gefahr oder zu Zwecken der Beweissicherung erforderlich ist und die Tatsache der Aufzeichnung für die Betroffenen durch geeignete Maßnahmen erkennbar gemacht wurde. Die Aufzeichnungen sind spätestens nach sieben Tagen zu löschen, es sei denn, die weitere Speicherung ist zur Aufklärung oder Verfolgung der dokumentierten Vorkommnisse erforderlich.

§ 38 Fernmess- und Fernwirkdienste

(1) Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen, insbesondere in der Wohnung oder in 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 des Betroffenen nach Absatz 1 abhängig gemacht werden. Verweigert oder widerruft der Betroffene seine Einwilligung, so dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen. Das Abschalten der Einrichtung durch den Betroffenen gilt im Zweifel als Widerruf der Einwilligung.

**Beschlüsse
des 2. Ausschusses**

Entwurf**Beschlüsse
des 2. Ausschusses****§ 39 Öffentliche Auszeichnungen**

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

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

Abschnitt 6**PERSONENBEZOGENE DATEN
EHEMALIGER EINRICHTUNGEN****Abschnitt 6 unverändert****§ 40 Zuständigkeit für personenbezogene
Daten ehemaliger Einrichtungen**

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

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

Entwurf

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

**§ 41 Zulässige Nutzung und
Zweckbestimmung der Speicherung
personenbezogener Daten ehemaliger
Einrichtungen**

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

**Abschnitt 7
STRAF-, ÜBERGANGS-
UND SCHLUSSVORSCHRIFTEN**

§ 42 Straftaten

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

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

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

**Beschlüsse
des 2. Ausschusses**

**Abschnitt 7
STRAF-, ÜBERGANGS-
UND SCHLUSSVORSCHRIFTEN**

§ 42 Straftaten

(1) unverändert

Entwurf	Beschlüsse des 2. Ausschusses
(2) Ebenso wird bestraft, wer	(2) Ebenso wird bestraft, wer
1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,	1. unverändert
2. entgegen § 15 Abs. 2 Satz 2 oder § 34 Abs. 4 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder	2. unverändert
3. entgegen § 34 Abs. 2 Satz <u>3</u> die Zuordnungsfunktion anwendet und dadurch die Betroffenen erkennbar macht.	3. entgegen § 34 Abs. 2 Satz 6 die Zuordnungsfunktion anwendet und dadurch die Betroffenen erkennbar macht.
(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.	(3) unverändert
(4) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind neben dem Betroffenen die Daten verarbeitende Stelle und der Landesbeauftragte für den Datenschutz.	(4) unverändert
§ 43 Übergangsvorschrift	§ 43 unverändert
Verarbeitungen personenbezogener Daten, die zum Zeitpunkt des In-Kraft-Tretens dieses Gesetzes bereits begonnen wurden, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.	

Entwurf	Beschlüsse des 2. Ausschusses
<p data-bbox="331 327 625 353" style="text-align: center;">§ 44 Außer-Kraft-Treten</p> <p data-bbox="180 405 778 622">(1) Mit In-Kraft-Treten dieses Gesetzes tritt das Landesdatenschutzgesetz von Mecklenburg-Vorpommern vom 24. Juli 1992 (GVOBl. M-V S. 487), geändert durch Artikel 2 des Gesetzes vom 7. Juli 1997 (GVOBl. M-V S. 282), außer Kraft.</p> <p data-bbox="180 667 778 734">(2) § 30 tritt am 31. Dezember 2004 außer Kraft.</p>	<p data-bbox="970 327 1184 353" style="text-align: center;">§ 44 unverändert</p>
<p data-bbox="309 808 651 869" style="text-align: center;">Artikel 2 Änderung anderer Rechtsvorschriften</p> <p data-bbox="180 913 778 1093">(1) Das Landeskrankenhausgesetz vom 8. Dezember 1993 (GVOBl. M-V S. 990), zuletzt geändert durch <u>das Gesetz vom 11. Dezember 1996</u> (GVOBl. M-V S. 635), wird wie folgt geändert:</p> <p data-bbox="180 1137 778 1205">1. Die Inhaltsübersicht wird wie folgt geändert:</p> <p data-bbox="225 1249 778 1317">a) Die Angabe zu § 16 wird folgt neu gefasst:</p> <p data-bbox="264 1361 778 1429" style="padding-left: 20px;">„§ 16 Nutzen und Übermitteln von Daten im Krankenhaus“</p> <p data-bbox="225 1473 778 1541">b) Die Angabe zu § 22 wird folgt neu gefasst:</p> <p data-bbox="264 1585 778 1615" style="padding-left: 20px;">„§ 22 (weggefallen)“</p>	<p data-bbox="906 808 1248 869" style="text-align: center;">Artikel 2 Änderung anderer Rechtsvorschriften</p> <p data-bbox="778 913 1372 1093">(1) Das Landeskrankenhausgesetz vom 8. Dezember 1993 (GVOBl. M-V S. 990), zuletzt geändert durch Artikel 3 des Gesetzes vom 6. Juli 2001 (GVOBl. M-V S. 249), wird wie folgt geändert:</p> <p data-bbox="778 1137 1372 1205">1. unverändert</p>

Entwurf	Beschlüsse des 2. Ausschusses
<p>2. § 14 Abs. 2 wird wie folgt neu gefasst:</p> <p>„(2) Ergänzend zu den Vorschriften dieses Gesetzes über die Verarbeitung von Patientendaten gelten die Vorschriften des Landesdatenschutzgesetzes vom 2001 (GVOBl. M-V S.) mit Ausnahme des § 25 Abs. 3 des Landesdatenschutzgesetzes und mit der Maßgabe, dass an die Stelle der §§ 4 und 7 Abs. 1 bis 4, der §§ 8 bis 10, des § 13 Abs. 2 bis 5 und der §§ 14, 15, 24 und 34 des Landesdatenschutzgesetzes die Vorschriften dieses Gesetzes treten. § 2 Abs. 5 des Landesdatenschutzgesetzes findet auf Krankenhäuser keine Anwendung.“</p>	2. unverändert
<p>3. § 16 wird wie folgt geändert:</p> <p>a) Die Überschrift wird wie folgt neu gefasst:</p> <p>„Nutzen und Übermitteln von Daten im Krankenhaus“</p> <p>b) In Absatz 4 Satz 1 werden die Wörter „verarbeitet und“ gestrichen.</p>	3. unverändert
<p>4. In § 17 Abs. 3 Satz 2 wird das Wort „öffentliche“ gestrichen und die Zahl „14“ durch die Zahl „16“ ersetzt.</p>	4. unverändert
<p>5. In § 20 Abs. 6 Satz 2 wird die Angabe „§ 17“ durch die Angabe „§§ 21 und 22“ ersetzt.</p>	5. unverändert
<p>6. § 22 wird aufgehoben.</p>	6. unverändert
<p>(2) In § 2 Abs. 2 Satz 1 des Krebsregisterausführungsgesetzes vom 29. Mai 1998 (GVOBl. M-V S. 512) wird das Wort „Meldung“ durch das Wort „Datenverarbeitung“ ersetzt.</p>	(2) unverändert

Entwurf	Beschlüsse des 2. Ausschusses
(3) § 5 des Insolvenzordnungsausführungsgesetzes vom 17. November 1999 (GVOBl. M-V S. 611) wird aufgehoben.	(3) unverändert
(4) Das Landespressegesetz für das Land Mecklenburg Vorpommern vom 6. Juni 1993 (GVOBl. M-V S. 541) wird wie folgt geändert:	(4) unverändert
1. Nach § 18 wird folgender § 18 a eingefügt:	
„§ 18 a Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Presse	
Soweit Unternehmen oder Hilfsunternehmen der Presse personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken erheben, verarbeiten oder nutzen, gelten von den Vorschriften des Bundesdatenschutzgesetzes nur die §§ 5, 9 und 38 a sowie § 7. Es wird allein für Schäden gehaftet, die durch eine Verletzung des Datengeheimnisses nach § 5 des Bundesdatenschutzgesetzes oder durch unzureichende technische oder organisatorische Maßnahmen i. S. d. § 9 des Bundesdatenschutzgesetzes eintreten.“	
2. In § 22 Abs. 1 Satz 2 werden vor „§ 131“ „§§ 86, 86a, 130“ eingefügt.	

Entwurf**Beschlüsse
des 2. Ausschusses**

(5) Das Sicherheits- und Ordnungsgesetz in der Fassung der Bekanntmachung vom 25. März 1998 (GVOBl. M-V S. 335), zuletzt geändert durch das Gesetz vom 24. Oktober 2001 (GVOBl. M-V S. 386) wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) In der Überschrift in Abschnitt 3 Unterabschnitt 3 wird das Wort „Errichtungsanordnung“ durch das Wort „Verfahrensverzeichnis“ ersetzt.

b) Die Angabe zu § 47 wird wie folgt neu gefasst:

„§ 47 Verfahrensverzeichnis“.

2. Nach § 3 Abs. 3 wird folgender Absatz 4 angefügt:

„(4) Im Sinne dieses Gesetzes ist

1. Datenerhebung:

das Beschaffen von Daten;

2. Datenverarbeitung:

das Speichern, Verändern, Übermitteln, Sperren, Löschen, Anonymisieren, Pseudonymisieren und Verschlüsseln von Daten;

3. Datennutzung:

die inhaltliche Auswertung und Verwendung von Daten.“.

3. § 25 Abs. 3 wird aufgehoben.

Entwurf**Beschlüsse
des 2. Ausschusses**

4. In § 42 Abs. 2 Satz 1 werden die Wörter „Die Errichtungsanordnung“ durch die Wörter „Das Verfahrungsverzeichnis“ ersetzt.
5. In § 45 Abs. 4 Satz 2 wird die Angabe „§ 30“ durch die Angabe „§ 34“ ersetzt.
6. In der Überschrift in Abschnitt 3 Unterabschnitt 3 wird das Wort „Errichtungsanordnung“ durch das Wort „Verfahrungsverzeichnis“ ersetzt.
7. § 47 wird wie folgt neu gefasst:

„§ 47 Verfahrungsverzeichnis

(1) Verfahren zum Umgang mit personenbezogenen Daten sind auf das erforderliche Maß zu beschränken. In angemessenen Abständen ist die Notwendigkeit ihrer Weiterführung oder Änderung zu prüfen.

(2) Für jedes automatisierte Verfahren ist ein Verfahrungsverzeichnis zu erstellen, in dem neben den Vorgaben des § 18 des Landesdatenschutzgesetzes zusätzlich Prüffristen nach § 46 anzuordnen sind.

(3) Das Innenministerium regelt das Nähere durch Verwaltungsvorschrift. Das Verfahrungsverzeichnis ist dem Landesbeauftragten für den Datenschutz zu übersenden.“.

8. In § 76 wird die Angabe „§ 23“ durch die Angabe „§ 27“ ersetzt.

Entwurf**Artikel 3 Neufassung des
Landeskrankenhausgesetzes**

Das Sozialministerium kann den Wortlaut des Landeskrankenhausgesetzes in der vom In-Kraft-Treten dieses Gesetzes an geltenden Fassung im Gesetz- und Verordnungsblatt für Mecklenburg-Vorpommern bekannt machen.

Artikel 4 In-Kraft-Treten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

**Beschlüsse
des 2. Ausschusses**

Artikel 3 unverändert

Artikel 4 unverändert

Bericht des Abgeordneten Siegfried Friese

I. Allgemeines

Der Landtag hat den Gesetzentwurf der Landesregierung, Entwurf eines Gesetzes zur Änderung datenschutzrechtlicher Vorschriften, auf Drucksache 3/2219 in seiner 66. Sitzung am 20. September 2001 beraten und zur federführenden Beratung an den Innenausschuss sowie zur Mitberatung an den Petitionsausschuss, den Rechtsausschuss und den Finanzausschuss überwiesen.

Der Innenausschuss hat den Gesetzentwurf in seiner 82. Sitzung am 4. Oktober 2001 beraten und in der 92. Sitzung am 5. Dezember 2001 den Landesbeauftragten für den Datenschutz dazu angehört. Die abschließende Beratung fand in der 95. Sitzung am 27. Februar 2002 statt.

II. Stellungnahmen der mitberatenden Ausschüsse

1. Petitionsausschuss

Der Petitionsausschuss hat den o. g. Gesetzentwurf beraten und in seiner 63. Sitzung am 28. November 2001 mehrheitlich bei Zustimmung seitens der Koalitionsfraktionen sowie Gegenstimmen seitens der Fraktion der CDU beschlossen, dem federführenden Innenausschuss die unveränderte Annahme des Gesetzentwurfes zu empfehlen, soweit es die Angelegenheiten des Petitionsausschusses betrifft.

2. Rechtsausschuss

Der Rechtsausschuss hat den vorgenannten Gesetzentwurf in seiner 60. Sitzung am 1. November 2001 sowie in der 63. Sitzung am 6. Dezember 2001 beraten und einstimmig die Annahme in unveränderter Fassung empfohlen.

3. Finanzausschuss

Der Finanzausschuss hat in seiner 108. Sitzung am 24. Januar 2002 den o. g. Gesetzentwurf beraten und aus finanzpolitischer Sicht bei einer Stimmenthaltung seitens der Fraktion der PDS einvernehmlich die unveränderte Annahme empfohlen mit der Maßgabe, da möglicherweise das Konnexitätsprinzip doch berührt sein könnte, einer nochmaligen Prüfung durch den Innenausschuss und der notwendigen Veranlassung des sich daraus Ergebenden.

III. Wesentliche Ergebnisse der Beratungen des Innenausschusses

1. Ergebnisse der Anhörung des Datenschutzbeauftragten

Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern hat darauf hingewiesen, dass die EG-Richtlinie eine unabhängige Behörde für die Kontrolle der Datenschutzbestimmungen sowohl im privaten als auch im öffentlichen Bereich verlange. Eine Aufsicht über die Einhaltung datenschutzrechtlicher Bestimmungen bei den Privaten durch das Innenministerium entspreche dem nicht, da das Innenministerium nicht unabhängig sei. Insbesondere stehe einer unabhängigen Kontrolle durch das Innenministerium die im Gesetzentwurf im § 30 Absatz 1 Satz 2 vorgesehene Oberaufsicht des Landesbeauftragten für den Datenschutz über den Datenschutz beim Innenministerium entgegen. Dadurch könne das Innenministerium die eigene Kontrolle der Privaten nicht unabhängig vornehmen. Auch ein Brief der Europäischen Kommission an den Berliner Beauftragten für Datenschutz vom 11. September 2001 stütze diese Auffassung. Dort werde ausdrücklich ausgeführt, dass die unabhängige Kontrolle der Datenschutzbestimmungen durch eine nicht weisungsgebundene und keinen politischen Instanzen unterstellte Behörde erfolgen müsse, die nicht ausschließlich durch die Exekutive bestellt werde. Entsprechend könne diese Datenschutzbehörde nicht im Ministerium angesiedelt sein und nicht der Rechtsaufsicht unterliegen. Der Datenschutzbeauftragte hat sich besonders gegen die in der Begründung zu § 30 normierte Ausnahme der Notare von den Kontrollbefugnissen des Landesbeauftragten für den Datenschutz gewandt. Eine solche Ausnahmeregelung für Notare sei abzulehnen, da das Notargeheimnis nicht zum Schutze der Notare, sondern zum Schutze der Bürger bestünde und mithin kein Grund für eine Ausnahme der Notare von den Datenschutzbestimmungen erkennbar sei. In jedem Fall könne eine Ausnahme von den Datenschutzbestimmungen nicht allein in der Gesetzesbegründung erfolgen.

2. Abstimmungsergebnis zum Gesetzentwurf

Der Ausschuss hat in seiner 95. Sitzung am 27. Februar 2002 dem Gesetzentwurf nach Annahme einiger Änderungsanträge insgesamt einvernehmlich bei Enthaltung der Fraktion der CDU zugestimmt.

Der Ausschuss hat in einer weiteren Abstimmung ebenfalls einvernehmlich bei Enthaltung der Fraktion der CDU eine Entschließung zu der datenschutzrechtlichen Kontrolle der Notare und einer Vereinheitlichung der Kontrollinstitutionen für den Datenschutz im privaten und öffentlichen Bereich angenommen. Die Fraktion der CDU hat ihre Enthaltung dahin gehend begründet, dass hinsichtlich der datenschutzrechtlichen Kontrolle der Notare die Bedeutung der Entschließung für die Rechtslage ungeklärt sei.

IV. Zu den einzelnen Bestimmungen

Zu Artikel 1

Der Ausschuss hat dem § 1 in unveränderter Form einstimmig zugestimmt.

Zu § 2 hatte die Fraktion der SPD beantragt, den Absatz 5 Satz 2 wie folgt neu zu fassen:

„Mit Ausnahme der Vorschriften über die Meldepflichten und die Aufsichtsbehörde (§§ 4 d, 4 e und 38) sind im Übrigen die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes vom 20. Dezember 1990 (BGBl. I S. 2954), zuletzt geändert durch Artikel 1 des Gesetzes vom 18. Mai 2001 (BGBl. I S. 904), einschließlich der §§ 43 und 44 anwendbar.“

Zur Begründung wurde auf die Notwendigkeit einer Anpassung an die am 23. Mai 2001 in Kraft getretenen Änderungen des Bundesdatenschutzgesetzes hingewiesen.

Der Ausschuss hat diesem Änderungsantrag einstimmig zugestimmt und den § 2 in der geänderten Fassung einstimmig angenommen.

Zu § 3 hatte die Fraktion der SPD beantragt, in Absatz 6 Satz 2 nach den Wörtern „Europäischen Union“ die Wörter „oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum“ einzufügen.

Diese Einbeziehung der EWR-Staaten trage der zum 1. Juli 2000 wirksam gewordenen Übernahme der EG-Datenschutzrichtlinie durch die EWR-Staaten Rechnung, aufgrund derer das Gebot des freien Datenverkehrs auch im Verhältnis zwischen EU-Staaten und den übrigen EWR-Staaten gelte.

Der Ausschuss hat diesem Änderungsantrag einstimmig zugestimmt.

Die Fraktion der SPD hatte des Weiteren beantragt, in § 3 Absatz 7 nach den Wörtern „Europäischen Union“ das Wort „und“ durch ein Komma zu ersetzen und nach den Wörtern „ihrer Mitgliedstaaten“ die Wörter „oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum“ einzufügen.

Auch insoweit wurde auf die Übernahme der EG-Datenschutzrichtlinie durch die EWR-Staaten hingewiesen.

Der Ausschuss hat den Änderungsantrag ebenfalls einstimmig angenommen und den geänderten § 3 einstimmig verabschiedet.

Den §§ 4 bis 8 hat der Ausschuss in unveränderter Form einstimmig zugestimmt.

Zu § 9 hatten die Fraktionen der SPD und PDS beantragt, in Absatz 3 Satz 1 die Wörter „und Nutzung“ zu streichen, weil in dem neu definierten Begriff „Verarbeitung“ die Nutzung bereits einbezogen sei.

Der Ausschuss hat diesem Änderungsantrag sowie dem geänderten § 9 einstimmig zugestimmt.

Der Ausschuss hat den unveränderten §§ 10 bis 15 des Gesetzentwurfes einstimmig zugestimmt.

Zu § 16 hatte die Fraktion der SPD beantragt, in Absatz 1 Satz 1 nach den Wörtern „Europäischen Union“ die Wörter „oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum“ einzufügen, um damit der Übernahme der EG-Datenschutzrichtlinie durch die EWR-Staaten Rechnung zu tragen.

Diesem Änderungsantrag hat der Ausschuss einvernehmlich mit den Stimmen der Fraktionen der SPD und PDS und einer Stimme der Fraktion der CDU, bei einer Enthaltung seitens der Fraktion der CDU zugestimmt.

Die Fraktion der SPD hatte des Weiteren beantragt, in Absatz 2 Satz 1 ebenfalls nach den Wörtern „Europäischen Union“ die Wörter „und der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum“ einzufügen, um auch dort der Übernahme der EG-Datenschutzrichtlinie durch die EWR-Staaten Rechnung zu tragen.

Der Ausschuss hat auch diesem Änderungsantrag sowie dem geänderten § 16 einvernehmlich mit den Stimmen der Fraktionen der SPD und PDS und einer Stimme der Fraktion der CDU, bei einer Enthaltung seitens der Fraktion der CDU zugestimmt.

Der Ausschuss hat den unveränderten §§ 17 bis 19 einstimmig zugestimmt.

Zu § 20 hatten die Fraktionen der SPD und PDS beantragt, Absatz 1 Satz 7 aufzuheben, da der hier enthaltene Verweis auf § 29 Absatz 8 ins Leere ginge, weil ein ursprünglich vorgesehenes Zeugnisverweigerungsrecht dort wegen fehlender Gesetzgebungskompetenz nicht normiert sei.

Der Ausschuss hat diesem Änderungsantrag einstimmig zugestimmt und den geänderten § 20 einvernehmlich mit den Stimmen der Fraktionen der SPD und PDS und einer Stimme der Fraktion der CDU, bei einer Enthaltung seitens der Fraktion der CDU angenommen.

Der Ausschuss hat die §§ 21 bis 23 einstimmig unverändert angenommen.

Zu § 24 hatte die Fraktion der SPD beantragt, die Absätze 3 und 4 zu streichen.

§ 24 Absatz 3 sei inhaltsgleich mit § 24 Absatz 6 und damit überflüssig und die Regelung in § 24 Absatz 4 berücksichtige noch nicht das im Gesetz aufgenommene Akteneinsichtsrecht und sei dahin gehend anzupassen und aus systematischen Gründen nach den Vorschriften über die Akteneinsicht einzuordnen.

Der Ausschuss hat diesen Änderungsantrag einstimmig angenommen.

Die Fraktion der SPD hatte ferner beantragt, die bisherigen Absätze 5 und 6 als Absätze 3 und 4 im Gesetz vorzusehen. Diesem Änderungsantrag hat der Ausschuss einstimmig zugestimmt.

Die Fraktion der SPD hatte ferner beantragt, einen neuen Absatz 5 mit folgendem Wortlaut anzufügen:

„(5) Die Ablehnung der Auskunftserteilung und die Versagung der Einsichtnahme bedürfen keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung oder der Versagung der Akteneinsicht verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.“

Dieser neue Absatz 5 sollte die bisher in Absatz 4 geregelten Ausschlussgründe für die Auskunftserteilung auch auf die Einsichtnahme erweitern.

Der Ausschuss hat diesen Änderungsantrag einstimmig angenommen.

Die Fraktion der SPD hatte ferner beantragt, die bisherigen Absätze 7 und 8 als die neuen Absätze 6 und 7 vorzusehen.

Der Ausschuss hat sowohl diesem Änderungsantrag als auch dem geänderten § 24 insgesamt einstimmig zugestimmt.

Der Ausschuss hat den unveränderten §§ 25 bis 29 einstimmig zugestimmt.

Zu § 30 hat der Ausschuss insbesondere über die in der Gesetzesbegründung niedergelegte Auffassung der Landesregierung diskutiert, nach der die Notare nicht der Kontrolle des Landesdatenschutzbeauftragten in datenschutzrechtlicher Hinsicht unterlägen. Aufgrund der Bedenken, diese Frage in der Gesetzesbegründung zu regeln, hat das Innenministerium einen Änderungsvorschlag vorgelegt, nach dem die Notare ausdrücklich von der datenschutzrechtlichen Kontrolle durch den Landesbeauftragten für den Datenschutz ausgenommen worden wären. Diesen Änderungsantrag hat sich jedoch keine Fraktion zu eigen gemacht, da übereinstimmend eine datenschutzrechtliche Kontrolle der Notare durch den Landesbeauftragten für den Datenschutz befürwortet wurde. Dabei haben sich die Fraktionen von SPD und PDS für eine Verabschiedung des ursprünglichen Gesetzestextes und die Annahme einer Entschließung ausgesprochen. Die Entschließung sollte klarstellen, dass bereits aufgrund der geltenden Rechtslage auch die Notare der datenschutzrechtlichen Kontrolle durch den Landesbeauftragten für den Datenschutz unterlägen.

Dagegen sprach sich die Fraktion der CDU grundsätzlich für eine gesetzliche Regelung aus, sah hier jedoch einen Vorrang der bundesrechtlichen Vorschriften über das Notargeheimnis. Wenn der Landtag zu dieser Frage nur eine Entschließung verabschiede, werde nach Auffassung der Fraktion der CDU die Entscheidung zu Lasten der Rechtssicherheit letztlich den Gerichten überlassen.

Im Ergebnis hat der Ausschuss dem unveränderten § 30 einvernehmlich bei Enthaltung seitens der Fraktion der CDU zugestimmt.

Der Ausschuss hat den unveränderten §§ 31 bis 41 einstimmig zugestimmt.

Zu § 42 hatte die Fraktion der SPD beantragt, in Absatz 2 Nummer 3 die Angabe „Satz 2“ durch die Angabe „Satz 6“ zu ersetzen, um einen fehlerhaften Verweis zu korrigieren.

Der Ausschuss hat diesem Änderungsantrag mit den Stimmen der Fraktionen der SPD und PDS bei Enthaltung seitens der Fraktion der CDU einvernehmlich zugestimmt und dem geänderten § 42 einvernehmlich mit den Stimmen der Fraktionen der SPD und PDS und einer Stimme der Fraktion der CDU, bei einer Enthaltung seitens der Fraktion der CDU zugestimmt.

Der Ausschuss hat den unveränderten §§ 43 bis 44 einstimmig zugestimmt und dem gesamten Artikel 1 in der geänderten Fassung einvernehmlich mit den Stimmen der Fraktionen der SPD und PDS und einer Stimme der Fraktion der CDU, bei einer Enthaltung seitens der Fraktion der CDU zugestimmt.

Zu Artikel 2

Zu Absatz 1 hatten die Fraktionen der SPD und PDS beantragt, in Satz 1 die Angabe „das Gesetz vom 11. Dezember 1996 (GVOBl. M-V S. 635)“ durch die Angabe „Artikel 3 des Gesetzes vom 6. Juli 2001 (GVOBl. M-V S. 249)“ zu ersetzen, da dieser Änderungshinweis zu aktualisieren sei.

Der Ausschuss hat diesem Änderungsantrag und dem geänderten Absatz 1 einstimmig zugestimmt.

Der Ausschuss hat den unveränderten Absätzen 2 bis 4 einstimmig zugestimmt.

Die Fraktionen der SPD und PDS hatten ferner die Anfügung eines Absatzes 5 beantragt, der folgenden Wortlaut erhalten sollte:

„(5) Das Sicherheits- und Ordnungsgesetz in der Fassung der Bekanntmachung vom 25. März 1998 (GVOBl. M-V S. 335), zuletzt geändert durch das Gesetz vom 24. Oktober 2001 (GVOBl. M-V S. 386) wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) In der Überschrift in Abschnitt 3 Unterabschnitt 3 wird das Wort ‚Errichtungsanordnung‘ durch das Wort ‚Verfahrensverzeichnis‘ ersetzt.

b) Die Angabe zu § 47 wird wie folgt neu gefasst:

‚§ 47 Verfahrensverzeichnis‘

2. Nach § 3 Abs. 3 wird folgender Absatz 4 angefügt:

‚(4) Im Sinne dieses Gesetzes ist

1. Datenerhebung:

das Beschaffen von Daten;

2. Datenverarbeitung:

das Speichern, Verändern, Übermitteln, Sperren, Löschen, Anonymisieren, Pseudonymisieren und Verschlüsseln von Daten;

3. Datennutzung:

die inhaltliche Auswertung und Verwendung von Daten.‘

3. § 25 Abs. 3 wird aufgehoben.

4. In § 42 Abs. 2 Satz 1 werden die Wörter ‚Die Errichtungsanordnung‘ durch die Wörter ‚Das Verfahrensverzeichnis‘ ersetzt.

5. In § 45 Abs. 4 Satz 2 wird die Angabe ‚§ 30‘ durch die Angabe ‚§ 34‘ ersetzt.

6. In der Überschrift in Abschnitt 3 Unterabschnitt 3 wird das Wort ‚Errichtungsanordnung‘ durch das Wort ‚Verfahrensverzeichnis‘ ersetzt.

7. § 47 wird wie folgt neu gefasst:

„§ 47 Verfahrensverzeichnis

(1) Verfahren zum Umgang mit personenbezogenen Daten sind auf das erforderliche Maß zu beschränken. In angemessenen Abständen ist die Notwendigkeit ihrer Weiterführung oder Änderung zu prüfen.

(2) Für jedes automatisierte Verfahren ist ein Verfahrensverzeichnis zu erstellen, in dem neben den Vorgaben des § 18 des Landesdatenschutzgesetzes zusätzlich Prüffristen nach § 46 anzuordnen sind.

(3) Das Innenministerium regelt das Nähere durch Verwaltungsvorschrift. Das Verfahrensverzeichnis ist dem Landesbeauftragten für den Datenschutz zu übersenden.“

8. In § 76 wird die Angabe ‚§ 23‘ durch die Angabe ‚§ 27‘ ersetzt.“

Zur Begründung war auf die Notwendigkeit der Anpassung der Begrifflichkeiten an die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates und auf die Überflüssigkeit des § 25 Absatz 3 im Hinblick auf die allgemeinen Kollisionsregeln hingewiesen worden.

Der Ausschuss hat diesem Änderungsantrag und dem geänderten Absatz 5 einstimmig zugestimmt.

Der Ausschuss hat dem geänderten Artikel 2 einstimmig zugestimmt.

Zu den Artikeln 3 und 4

Der Ausschuss hat den unveränderten Artikeln 3 und 4 einstimmig zugestimmt.

Zur Entschließung

Die Fraktionen der SPD und PDS hatten des Weiteren die Annahme folgender Entschließung beantragt:

„Hinsichtlich der Regelung in § 30 geht der Landtag davon aus, dass Notare als unabhängige Träger eines öffentlichen Amtes der Datenschutzkontrolle durch den Landesbeauftragten für den Datenschutz unterliegen.

Der Landtag geht davon aus, dass die Landesregierung prüft, die Datenschutzkontrolle im öffentlichen und privaten Bereich institutionell einheitlich zu regeln.“

Der Ausschuss hat diesem Entschließungsantrag einvernehmlich mit den Stimmen der Fraktionen der SPD und PDS bei Enthaltung der Fraktion der CDU angenommen.

Der Ausschuss hat anlässlich der Stellungnahme des Finanzausschusses die Frage der Konnexität erörtert, jedoch bei diesem Gesetzentwurf keinen Fall der Konnexität festgestellt.

Schwerin, den 6. März 2002

Siegfried Friese
Berichterstatter