

Berliner
Datenschutzbeauftragter

BERLIN

DATEN SCHUTZ

Berliner Informationsgesetzbuch
Teil 1 – Heft 1

Berliner Datenschutzgesetz

Berliner Informationsgesetzbuch
Teil 1 : Datenschutzgesetze
Heft 1

Berliner Datenschutzgesetz

3. Auflage: Berlin · August 1995

Im Berliner Informationsgesetzbuch sind bisher erschienen:

Teil 1: Datenschutzgesetze

Heft 1 – Berliner Datenschutzgesetz

Heft 2 – Bundesdatenschutzgesetz

Teil 2: Sicherheits- und Ordnungsrecht

Heft 1 – Allgemeines Sicherheits- und Ordnungsgesetz

Heft 2 – Meldegesetz

Teil 3: Gesundheits- und Sozialrecht

Heft 1 – Schutz der Sozialdaten

Impressum

Herausgeber: Berliner Datenschutzbeauftragter
verantwortlich: Claudia Schmid
Pallasstraße 25/26, 10781 Berlin
Telefon: (0 30) 7 83 88 44
(ab Oktober 1995: + 78 76 88 44)
Telefax: (0 30) 2 16 99 27
Bildschirmtext: *92 67 90 #

Redaktion,
Layout: Volker Brozio

Druck: Verwaltungsdruckerei Berlin
gedruckt auf Umwelt-Recycling-Papier
3. Auflage: August 1995

Vorwort

Die Forderung des Bundesverfassungsgerichts, die Verarbeitung personenbezogener Daten in der öffentlichen Verwaltung normenklar zu regeln, hat dazu geführt, daß sich datenschutzrechtliche Regelungen inzwischen in einer Vielzahl von Gesetzen wiederfinden.

Gerade das Berliner Datenschutzgesetz, das den Datenschutz für Behörden und andere öffentliche Stellen des Landes Berlins regelt, nimmt diese Forderung sehr ernst und läßt die Erhebung, aber auch andere Formen der Datenverarbeitung nur noch zu, wenn eine derartige spezialrechtliche Rechtsgrundlage besteht.

Die Voraussetzung für die Verarbeitung personenbezogener Daten, die in allen Verwaltungen gleichermaßen anfallen und die nicht wie das Personal- und Haushaltswesen gesondert geregelt sind, sind im Gesetz über die Informationsverarbeitung bei der allgemeinen Verwaltungstätigkeit (Informationsverarbeitungsgesetz – IVG) festgelegt.

Mit der Novellierung des Berliner Datenschutzgesetzes vom 22. Juni 1995 dürfen personenbezogene Daten nunmehr ohne ein spezielles Gesetz auch dann verarbeitet werden, wenn wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Seither sind bei der Ausführung von Bundesrecht auch die Bestimmungen des Bundesdatenschutzgesetzes anwendbar. Die vorliegende Ausgabe des Berliner Datenschutzgesetzes gibt die Fassung des Gesetzes nach dieser Novellierung wieder, bei der im übrigen dem Berliner Datenschutzbeauftragten auch die Aufgabe der Kontrolle bei der privaten Datenverarbeitung übertragen wurde.

Dieses Heft ist Teil der Sammlung „Berliner Informationsgesetzbuch“, in der wir Schritt für Schritt alle in Berlin geltenden datenschutzrechtlichen Regelungen zusammentragen wollen. Die Bezeichnung ist ein Hinweis darauf, daß die Informationsgesellschaft nicht nur durch ein rasant anwachsendes informationstechnisches Arsenal geprägt ist, sondern auch einer entsprechenden Vielfalt informationsrechtlicher Regelungen bedarf.

In der gleichen Aufmachung liegen bisher Texte des Bundesdatenschutzgesetzes, des Allgemeinen Sicherheits- und Ordnungsgesetzes, des Berliner Meldegesetzes sowie der Regelungen zum Sozialdatenschutz vor. Ein einfacher Einband, mit dessen Hilfe die Bände zu einem handlichen Informationsgesetzbuch zusammengeführt werden können, kann von uns bezogen werden.

Nach wie vor nehmen wir gerne Anregungen auf, um welche Vorschriften oder andere Texte die Sammlung ergänzt werden könnte.

Dr. Hansjürgen Garstka
Berliner Datenschutzbeauftragter

<h1>Inhalt</h1>

	Seite
1. Einleitung	5
2. Berliner Datenschutzgesetz	7
3. Informationsverarbeitungsgesetz	29

1. Einleitung

Vor zehn Jahren hat das Bundesverfassungsgericht ein bahnbrechendes Urteil gefällt: In dem sogenannten Volkszählungsurteil vom Dezember 1983 wurde der Datenschutz als Grundrecht der Bürger anerkannt. Das höchste deutsche Gericht hat klargestellt, daß in das „informationelle Selbstbestimmungsrecht“ nur eingegriffen werden darf, wenn es zum Schutz öffentlicher Interessen unerlässlich ist. Das Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann er wem welche Informationen offenbart, darf nur durch präzise und klare gesetzliche Regelungen beschränkt werden.

Das am 10. November 1990 in Kraft getretene neue Berliner Datenschutzgesetz hat die Forderungen des Bundesverfassungsgerichts konsequent umgesetzt und stellt eines der fortschrittlichsten und bürgerfreundlichsten Gesetze auf diesem Gebiet dar.

Das Berliner Datenschutzgesetz gilt allerdings nur für die Behörden und sonstigen öffentlichen Stellen des Landes Berlin. Hierzu zählen die Senats- und Bezirksverwaltungen mit den ihnen nachgeordneten Einrichtungen (z. B. Polizeipräsident in Berlin, Landesamt für Verfassungsschutz, Krankenhäuser, Schulen), aber auch dem Land zugeordnete Einrichtungen mit eigener Rechtspersönlichkeit (z. B. Hochschulen, Kammern). Für die Datenverarbeitung nicht öffentlicher Stellen, wie z. B. Banken, Versicherungen, private Arbeitgeber, finden die Regelungen des Bundesdatenschutzgesetzes Anwendung.

Dies sind die wichtigsten Neuregelungen im Berliner Datenschutzgesetz:

- Jeder Bürger hat Anspruch auf gebührenfreie Auskunft über die zu seiner Person gespeicherten Daten, Zweck und Rechtsgrundlage der Verarbeitung, die Herkunft der Daten und die Empfänger von Übermittlungen innerhalb der letzten 2 Jahre (§ 16 Abs. 1). Darf die Auskunft ausnahmsweise verweigert werden (§ 16 Abs. 5), sind die wesentlichen Gründe dem Betroffenen im einzelnen mitzuteilen.
- Die Datenschutzbestimmungen gelten für jede Form der Datenverarbeitung. Es macht keinen Unterschied mehr, ob die Daten sich in Dateien oder Akten befinden. Folgerichtig wurde auch ein Recht auf Akteneinsicht vorgesehen (§ 16 Abs. 4).
- Eine Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine besondere Rechtsvorschrift außerhalb des Datenschutzgesetzes sie erlaubt oder der Betroffene eingewilligt hat (§ 6 Abs. 1). Auch die besondere, bereichsspezifische Regelung rechtfertigt die Datenverarbeitung nur dann, wenn sie eine dem Berliner Datenschutzgesetz vergleichbare Regelung trifft. Seither ist eine Vielzahl solcher Gesetze verabschiedet worden.
- Um die Transparenz der Datenverarbeitung zu gewährleisten, sind personenbezogene Daten grundsätzlich beim Betroffenen selbst zu erheben und nicht hinter seinem Rücken (§ 10 Abs. 1).
- Erstmals gesetzlich verankert wurde der Grundsatz der Zweckbindung, der die datenverarbeitenden Stellen verpflichtet, personenbezogene Daten grundsätzlich nur zu dem Zweck zu nutzen, zu dem sie die Daten erlangt haben. Ausnahmen hiervon sind nur mit ausdrücklicher Einwilligung des Betroffenen oder einer besonderen gesetzlichen Regelung zulässig (§ 11).

- Wird jemand durch rechtswidrige Datenverarbeitung in seinen schutzwürdigen Belangen beeinträchtigt, hat ihm die öffentliche Stelle, die die Daten verarbeitet hat, den entstandenen Vermögensschaden zu ersetzen, ohne summenmäßige Begrenzung und ohne daß ihr ein Verschulden nachgewiesen werden muß. In schweren Fällen kann der Betroffene auch ein Schmerzensgeld verlangen (§ 18 Abs. 1).
- Werden personenbezogene Daten in Dateien aufgenommen, haben die datenverarbeitenden Stellen bis auf eng begrenzte Ausnahmen (§ 19 Abs. 3) Dateibeschreibungen zu erstellen, in denen insbesondere der Kreis der Betroffenen, regelmäßige Datenübermittlungen und Lösungsfristen festzulegen sind (§ 19 Abs. 2). Diese Dateibeschreibungen kann jeder in einem Register beim Berliner Datenschutzbeauftragten einsehen (§ 25).
- Die interne Kontrolle der Datenverarbeitung soll durch behördliche Datenschutzbeauftragte erfolgen (§ 19 Abs. 5). Sie haben auch dafür zu sorgen, daß ein Verzeichnis der Geräte, der verwendeten Betriebssysteme sowie der Standard- und Anwenderprogramme geführt wird (§ 19 Abs. 4).

2. Berliner Datenschutzgesetz

Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz – BlnDSG)

**in der Fassung vom 17. Dezember 1990 (GVBl. 1991, S. 16, 54),
zuletzt geändert durch Gesetz vom 3. Juli 1995
(GVBl. 1995, S. 404)**

Erster Abschnitt Allgemeine Vorschriften

§ 1

Aufgabe und Gegenstand des Datenschutzes

(1) Aufgabe dieses Gesetzes ist es, die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen zu regeln, um

1. das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind (informationelles Selbstbestimmungsrecht),
2. die auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Ordnung vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

(2) Dieses Gesetz schützt personenbezogene Daten, die von Behörden oder sonstigen öffentlichen Stellen erhoben, gespeichert, verändert, übermittelt, gespart, gelöscht oder sonst genutzt werden.

§ 2

Anwendungsbereich

(1) Zum Schutz personenbezogener Daten nach Maßgabe dieses Gesetzes sind alle Behörden und sonstigen öffentlichen Stellen (insbesondere nichtrechtsfähige Anstalten, Krankenhausbetriebe, Eigenbetriebe und Gerichte) des Landes Berlin und der landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (§ 28 des Allgemeinen Zuständigkeitsgesetzes) verpflichtet. Dies gilt auch für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

Anmerkungen:

Anmerkungen:

(2) Für landesunmittelbare Anstalten des öffentlichen Rechts, die am Wettbewerb teilnehmen, gelten die §§ 3, 6, 9 bis 17 und 30 dieses Gesetzes nicht. Für sie gelten die §§ 11, 27 Abs. 2, 28 bis 31, 33 bis 35, 39, 40 und 44 des Bundesdatenschutzgesetzes.

(3) Soweit personenbezogene Daten im Anwendungsbereich des Gesetzes über das Verfahren der Berliner Verwaltung verarbeitet werden, gelten die Vorschriften des Berliner Datenschutzgesetzes.

(4) Dieses Gesetz regelt den Schutz personenbezogener Daten für die Behörden und sonstigen öffentlichen Stellen umfassend. Andere Landesgesetze können für bestimmte Behörden und sonstige öffentliche Stellen einzelne notwendige Abweichungen von diesem Gesetz vorschreiben; im übrigen richtet sich der Datenschutz auch in diesen Fällen nach den Vorschriften dieses Gesetzes.

§ 3

Verarbeitung personenbezogener Daten im Auftrag

(1) Die Vorschriften dieses Gesetzes gelten für die Behörden und sonstigen öffentlichen Stellen auch insoweit, als personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. In diesen Fällen ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 5 Abs. 1) sorgfältig auszuwählen.

(2) Für die Behörden und sonstigen öffentlichen Stellen gelten die §§ 9 bis 17 dieses Gesetzes nicht, soweit sie personenbezogene Daten im Auftrag verarbeiten. In diesen Fällen ist die Verarbeitung personenbezogener Daten nur im Rahmen der Weisungen des Auftraggebers zulässig. Weisungen, die sich auf eine Datenverarbeitung richten, die gegen dieses Gesetz oder andere Rechtsvorschriften über den Datenschutz verstoßen, sind nicht auszuführen. Der Auftraggeber sowie dessen Aufsichtsbehörde sind unverzüglich zu unterrichten. Dasselbe gilt, wenn Daten verarbeitet werden sollen, die nach Ansicht des Auftragnehmers unter Verstoß gegen Rechtsvorschriften erlangt worden sind.

(3) Für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Land Berlin oder einer landesunmittelbaren Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, gelten die Vorschriften des Vierten Abschnittes entsprechend, soweit sie in den Fällen des Absatzes 1 Satz 1 im Auftrag tätig werden. Hinsichtlich der Befugnisse nach § 28 Abs. 1 wird das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes, Artikel 19 Abs. 2 Satz 1 der Verfassung von Berlin) für die Betriebs- und Geschäftszeit eingeschränkt.

(4) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Vorschriften dieses Gesetzes befolgt und sich, sofern die Daten-

verarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Berliner Datenschutzbeauftragten unterwirft. Wird die Datenverarbeitung in einem anderen Bundesland durchgeführt, ist sicherzustellen, daß sich der Auftragnehmer der Kontrolle des jeweiligen Landesbeauftragten unterwirft. Der Auftraggeber hat den Datenschutzbeauftragten und die Aufsichtsbehörde nach § 33 Abs. 1 dieses Gesetzes über die Beauftragung zu unterrichten.

§ 4

Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Entsprechendes gilt für Daten über Verstorbene, es sei denn, daß schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.

(2) Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Im Sinne der nachfolgenden Vorschriften ist

1. Erheben das Beschaffen von Daten über den Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger,
3. Verändern das inhaltliche Umgestalten gespeicherter Daten, ungeachtet der dabei angewendeten Verfahren,
4. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, daß die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder daß der Dritte zum Abruf bereitgehaltene Daten abrufen,
5. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten,
6. Löschen das Beseitigen gespeicherter Daten,
7. Nutzen jede sonstige Verwendung personenbezogener Daten.

(3) Im Sinne dieses Gesetzes ist

1. datenverarbeitende Stelle jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten läßt; nimmt diese unterschiedliche gesetzliche Aufgaben wahr, gilt diejenige Organisationseinheit als datenverarbeitende Stelle, der die Aufgabe zugewiesen ist;
2. Dritter jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen der Nummer 1 im Geltungsbereich des Grundgesetzes im Auftrag tätig werden;

Anmerkungen:

Anmerkungen:

3. eine Datei eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei) oder eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei);
4. eine Akte jede sonstigen amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger.

§ 5

Technische und organisatorische Maßnahmen

(1) Jede Behörde oder sonstige öffentliche Stelle, die für sich oder im Auftrag personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die Beachtung der in Absatz 3 genannten Anforderungen, zu gewährleisten. Die Art und Weise der Maßnahmen richtet sich nach dem jeweiligen Stand der Technik.

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

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

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. zu verhindern, daß Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. die Benutzung von Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte zu verhindern (Benutzerkontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
6. aufzuzeichnen, an welche Stellen wann welche personenbezogenen Daten übermittelt worden sind (Übermittlungs-kontrolle),
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu gewährleisten, daß bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(4) Der Senat setzt durch Rechtsverordnung die in Absatz 2 und 3 genannten Anforderungen nach dem jeweiligen Stand der Technik fest. Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Gewährleistung der Durchführung dieses Gesetzes gesichert erscheinen läßt. Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg im Betrieb erprobt worden sind.

Zweiter Abschnitt

Voraussetzungen der Datenverarbeitung und Rechte der Betroffenen

§ 6

Zulässigkeit der Datenverarbeitung

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

1. dieses Gesetz oder
2. eine besondere Rechtsvorschrift sie erlauben oder
3. der Betroffene eingewilligt hat.

Die Verarbeitung personenbezogener Daten ist nach diesem Gesetz zulässig, wenn wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Satz 1 Nr. 2 gilt nur, wenn die Rechtsvorschrift einen diesem Gesetz vergleichbaren Datenschutz gewährleistet.

(2) Werden aufgrund einer Rechtsvorschrift des Bundes personenbezogene Daten verarbeitet, ohne daß die Verarbeitung im einzelnen geregelt ist, finden die §§ 13–15 des Bundesdatenschutzgesetzes Anwendung.

(3) Wird die Datenverarbeitung auf die Einwilligung des Betroffenen gestützt, so ist dieser in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten sowie den Zweck der Übermittlung. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann.

Anmerkungen:

Anmerkungen:

(4) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist der Betroffene darauf schriftlich besonders hinzuweisen.

(5) Die Einwilligung ist unwirksam, wenn sie durch Androhung ungesetzlicher Nachteile oder durch fehlende Aufklärung bewirkt wurde.

§ 7

Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft und Benachrichtigung über die zu seiner Person gespeicherten Daten (§ 16),
2. Berichtigung, Sperrung oder Löschung der zu seiner Person gespeicherten Daten (§ 17),
3. Schadenersatz und Unterlassung (§ 18),
4. Anrufung des Datenschutzbeauftragten (§ 27),
5. Einsicht in das beim Berliner Datenschutzbeauftragten geführte Register (§ 25).

§ 8

Datengeheimnis

(1) Dienstkräften von Behörden und sonstigen öffentlichen Stellen, die Daten für sich oder im Auftrag verarbeiten, ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten.

(2) Die Dienstkräfte sind bei der Aufnahme ihrer Tätigkeit nach Maßgabe des Absatzes 1 zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

§ 9

Erforderlichkeit

(1) Nach Maßgabe der nachfolgenden Vorschriften ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der datenverarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.

(2) Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, so sind die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, über Absatz 1 hinaus zulässig. Diese Daten unterliegen insoweit einem Verwertungsverbot.

§ 10

Erheben

(1) Personenbezogene Daten sind unter der Voraussetzung des § 6 Abs. 1 grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben.

(2) Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist er in geeigneter Weise über den Zweck der Datenerhebung aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden Daten bei dem Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, so ist er auf die Rechtsgrundlage hinzuweisen. Im übrigen ist er darauf hinzuweisen, daß er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, so ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

(3) Bei Behörden und sonstigen öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn

1. eine Rechtsvorschrift dies erlaubt,
2. der Betroffene in diese Form der Erhebung eingewilligt hat oder
3. eine rechtzeitige Kenntnisgabe an den Betroffenen nicht möglich ist und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden könnten.

(4) Beim Betroffenen und bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn eine Rechtsvorschrift dieses vorsieht.

(5) Werden Daten beim Betroffenen ohne seine Kenntnis erhoben, so ist er davon zu benachrichtigen, sobald die rechtmäßige Erfüllung der Aufgaben dadurch nicht mehr gefährdet wird. Die Benachrichtigung umfaßt die Angabe der Rechtsgrundlage und die in Absatz 2 Satz 1 und 2 vorgesehene Aufklärung.

§ 11

Zweckbindung

(1) Personenbezogene Daten dürfen grundsätzlich nur zu dem Zweck weiterverarbeitet werden, zu dem sie erhoben oder gespeichert worden sind. Personenbezogene Daten, von denen eine Behörde oder sonstige öffentliche Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, so ist dies nur zulässig, wenn eine der Voraussetzungen des § 6 Abs. 1 vorliegt.

(3) Sind personenbezogene Daten in Akten derart verbunden, daß ihre Trennung nach verschiedenen Zwecken auch durch Vielfältigen und Unkenntlichmachen nicht oder nur mit unvertretbar großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe des Absatzes 2 für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen.

(4) Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefug-

Anmerkungen:

Anmerkungen:

nissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse unverzichtbar ist. Zu Aus- und Fortbildungszwecken dürfen personenbezogene Daten nur verwendet werden, wenn dies unerlässlich ist und schutzwürdige Belange des Betroffenen dem nicht entgegenstehen; zu Test- und Prüfungszwecken dürfen personenbezogene Daten nicht verwendet werden.

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

§ 12

Datenübermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ist zulässig, wenn eine der Voraussetzungen des § 6 Abs. 1 vorliegt. Werden die Daten vom Empfänger zur Erfüllung des gleichen Zwecks benötigt, zu dem die Daten erhoben worden sind, ist die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ferner zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der übermittelnden Stelle oder dem Empfänger zugewiesenen Aufgabe erforderlich ist.

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

(3) Über die Zulässigkeit der Datenübermittlung entscheidet die übermittelnde Stelle.

§ 13

Datenübermittlung an Stellen
außerhalb des öffentlichen Bereichs

Die Übermittlung personenbezogener Daten an Personen und andere Stellen außerhalb des öffentlichen Bereichs sowie an landesunmittelbare Anstalten des öffentlichen Rechts, die am Wettbewerb teilnehmen, ist zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.

§ 14

Datenübermittlung an öffentliche Stellen
außerhalb des Geltungsbereichs des Grundgesetzes

(1) Die Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- oder zwischenstaatliche Stellen ist zulässig, soweit die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaften oder einer internationalen Vereinbarung ausdrücklich geregelt ist.

(2) Eine Übermittlung ist auch zulässig, wenn für den Empfänger gleichwertige Datenschutzregelungen gelten und bei einer Übermittlung an öffentliche Stellen die Voraussetzungen der §§ 9 und 11 erfüllt sind. Die Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß sie gegen den Zweck eines deutschen Gesetzes, insbesondere gegen § 1 Abs. 1, verstoßen würde.

Anmerkungen:

§ 15

Automatisiertes Abrufverfahren

(1) Ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte darf durch Behörden oder sonstige öffentliche Stellen nur eingerichtet werden, wenn ein Gesetz dies ausdrücklich zuläßt. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Der Senat setzt durch Rechtsverordnung die Einzelheiten bei der Einrichtung automatisierter Abrufverfahren fest. Der Berliner Datenschutzbeauftragte ist vorher zu hören. Die Rechtsverordnung hat den Datenempfänger, die Datenart und den Zweck des Abrufs festzulegen. Sie hat Maßnahmen zur Datensicherung und zur Kontrolle vorzusehen, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

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

(4) Die Absätze 1 und 3 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offenstehen oder deren Veröffentlichung zulässig wäre.

§ 16

Auskunft und Benachrichtigung

(1) Werden personenbezogene Daten in einer Datei gespeichert, so ist dem Betroffenen von der datenverarbeitenden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Herkunft der Daten und die Empfänger von Übermittlungen innerhalb der letzten zwei Jahre.

(2) Werden personenbezogene Daten in einer automatisierten Datei gespeichert, so ist der Betroffene von dieser Tatsache schriftlich zu benachrichtigen. Die Benachrichtigung umfaßt einen Hinweis auf die Dateibeschriftung nach § 19 Abs. 2 sowie die Meldung zum Dateienregister nach § 25 Abs. 1 außer in den Fällen des § 25 Abs. 1 Sätze 5 und 7. Die Benachrichtigung kann zusammen mit der Erhebung erfolgen.

(3) Die Absätze 1 und 2 gelten nicht für personenbezogene Daten, die ausschließlich zum Zweck der Datensicherung gespeichert sind.

Anmerkungen:

(4) Sind personenbezogene Daten in Akten gespeichert, so kann der Betroffene bei der datenverarbeitenden Stelle Einsicht in die Akten verlangen. Werden die Akten zur Person des Betroffenen geführt, so hat er sie zu bezeichnen. Werden die Akten nicht zur Person des Betroffenen geführt, so hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, daß ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist; in diesem Fall ist dem Betroffenen Auskunft nach Absatz 1 zu erteilen. Im übrigen kann mit Einwilligung des Betroffenen statt Einsicht Auskunft gewährt werden. § 29 Abs. 1 und 3 des Verwaltungsverfahrensgesetzes bleibt unberührt.

(5) Die Absätze 1, 2 und 4 gelten nicht, soweit eine Abwägung ergibt, daß die dort gewährten Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten müssen; die wesentlichen Gründe sind dem Betroffenen im einzelnen mitzuteilen. Die Entscheidung trifft der Leiter der datenverarbeitenden Stelle oder dessen Stellvertreter. Werden Auskunft oder Einsicht nicht gewährt, so ist der Betroffene darauf hinzuweisen, daß er sich an den Berliner Datenschutzbeauftragten wenden kann. Die datenverarbeitende Stelle muß dem Datenschutzbeauftragten die Gründe der Auskunfts- oder Einsichtsverweigerung darlegen.

§ 17

Berichtigung, Sperrung und Löschung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Der Betroffene ist vor der Berichtigung zu hören.

(2) Personenbezogene Daten sind zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und solange sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Sie sind ferner zu sperren, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken oder zur Behebung einer bestehenden Beweisnot unerlässlich ist und der Betroffene in die Nutzung eingewilligt hat.

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

Satz 2 der Betroffene verlangt. In den Fällen des Satzes 2 1. Alternative ist der Betroffene vor der Löschung zu hören. Das gleiche gilt, wenn die Daten ohne Beteiligung des Betroffenen erhoben wurden und eine Benachrichtigung nach § 10 Abs. 5 nicht erfolgt ist.

(4) In den Fällen des Absatzes 2 Satz 2 und des Absatzes 3 Satz 1 und 2 kann die datenverarbeitende Stelle die Daten anstelle der dort vorgeschriebenen Sperrung oder Löschung einem dem öffentlichen Recht unterliegenden Archiv überantworten. Dazu ist die Einwilligung des Betroffenen in den Fällen des Absatzes 3 Satz 2 erforderlich.

(5) Von der Berichtigung nach Absatz 1, der Sperrung nach Absatz 2 und der Löschung nach Absatz 3 sind unverzüglich die Stellen zu verständigen, denen die Daten im Rahmen regelmäßiger Datenübermittlung übermittelt wurden.

(6) Sind personenbezogene Daten in Akten gespeichert und ist eine Sperrung nicht durch Vervielfältigen und Unkenntlichmachen möglich, so ist die Sperrung nach Absatz 2 Satz 2 nur durchzuführen, wenn die gesamte zur Person des Betroffenen geführte Akte zur Erfüllung der dort genannten Aufgaben nicht mehr erforderlich ist. Die Löschung nach Absatz 3 Satz 1 kann der Betroffene in diesem Fall nicht verlangen.

§ 18

Schadenersatz- und Unterlassungsanspruch

(1) Wird der Betroffene durch eine nach diesem Gesetz oder anderen Rechtsvorschriften über den Datenschutz rechtswidrige Datenverarbeitung in seinen schutzwürdigen Belangen beeinträchtigt, so hat ihm diejenige Behörde oder sonstige öffentliche Stelle, die die Daten verarbeitet oder nach § 3 Abs. 1 verarbeitet läßt, den daraus entstandenen Vermögensschaden zu ersetzen. Sind weitere Rechtsverletzungen zu besorgen, so kann der Betroffene Unterlassung verlangen. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen.

(2) Schadenersatz- und Unterlassungsansprüche auf Grund anderer Vorschriften bleiben unberührt.

§ 19

Durchführung des Datenschutzes, Dateibeschreibung und behördliche Datenschutzbeauftragte

(1) Die datenverarbeitenden Stellen, in den Fällen des § 4 Abs. 3 Nr. 1 Halbsatz 2 auch die jeweiligen Behörden oder sonstigen öffentlichen Stellen, und die Aufsichtsbehörden haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Sie haben insbesondere dafür zu sorgen, daß die ordnungs-

Anmerkungen:

Anmerkungen:

gemäß Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, gewährleistet ist.

(2) Die datenverarbeitenden Stellen haben für jede Datei in einer Beschreibung schriftlich festzulegen

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

(3) Absatz 2 findet keine Anwendung auf nichtautomatisierte Dateien, aus denen keine Daten an Dritte übermittelt werden, und auf Dateien, die bei automatisierter Verarbeitung ausschließlich aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden.

(4) Die datenverarbeitende Stelle oder die in ihrem Auftrag tätige Stelle ist verpflichtet, in einem Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, festzulegen

1. den Typ und die Art der Geräte,
2. den Hersteller,
3. die Anzahl und den Standort der Geräte,
4. das verwendete Betriebssystem,
5. die Möglichkeiten zur Datenfernverarbeitung und Datenübertragung und
6. verwendete Standard- und Anwenderprogramme.

Das Verzeichnis ist laufend auf dem neuesten Stand zu halten. Weitere in das Verzeichnis aufzunehmende Angaben über die Ausstattung der Geräte und deren Verwendung bestimmt der Senat durch Rechtsverordnung.

(5) Zur Wahrnehmung dieser Aufgaben bestellen die Behörden und sonstigen öffentlichen Stellen Datenschutzbeauftragte (behördliche Datenschutzbeauftragte). Für sie gelten die § 36 und § 37 des Bundesdatenschutzgesetzes entsprechend.

Dritter Abschnitt
Daten für das Abgeordnetenhaus
und die Bezirksverordnetenversammlungen

§ 20

(1) Die Behörden und sonstigen öffentlichen Stellen haben dem Abgeordnetenhaus, dessen verfassungsmäßigen Organen und den Fraktionen des Abgeordnetenhauses die von diesen im Rahmen ihrer Aufgaben verlangten Auskünfte über Daten zu erteilen. Personenbezogene Daten dürfen an diese Institutionen zur Erfüllung ihrer Aufgaben nur herausgegeben werden, wenn die in § 28 Abs. 2 Nr. 1 Satz 1 Buchstabe b und Satz 2 des Bundesdatenschutzgesetzes genannten Voraussetzungen erfüllt sind.

(2) Dieselbe Verpflichtung besteht gegenüber den Bezirksverordnetenversammlungen, ihren verfassungsmäßigen Organen und ihren Fraktionen, soweit diese im Rahmen ihrer Zuständigkeiten Auskünfte über Daten verlangen.

(3) Gesetzesvorlagen müssen Angaben über die Daten, die für den Vollzug des Gesetzes mit Datenverarbeitungsanlagen erforderlich sind, und über die Form der vorgesehenen Datenverarbeitung enthalten.

Vierter Abschnitt
Berliner Datenschutzbeauftragter

§ 21

Bestellung und Entlassung

(1) Der Berliner Datenschutzbeauftragte wird auf Vorschlag des Senats vom Abgeordnetenhaus mit den Stimmen der Mehrheit seiner Mitglieder gewählt und vom Senat ernannt.

(2) Der Datenschutzbeauftragte leistet vor dem Präsidenten des Abgeordnetenhauses folgenden Eid:

„Ich schwöre, mein Amt gerecht und unparteiisch getreu dem Grundgesetz, der Verfassung von Berlin und den Gesetzen zu führen und meine ganze Kraft dafür einzusetzen, so wahr mir Gott helfe.“

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Datenschutzbeauftragten beträgt fünf Jahre; nach dem Ende der Amtszeit bleibt er auf Aufforderung des Präsidiums des Abgeordnetenhauses bis zur Ernennung eines Nachfolgers im Amt. Die Wiederwahl ist zulässig. Vor Ablauf seiner Amtszeit kann der Datenschutzbeauftragte gegen seinen Willen nur entlassen werden, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.

§ 22

Rechtsstellung

(1) Der Datenschutzbeauftragte steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis.

Anmerkungen:

Anmerkungen:

(2) Der Datenschutzbeauftragte wird als oberste Landesbehörde eingerichtet; er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Präsidenten des Abgeordnetenhauses.

(3) Der Datenschutzbeauftragte darf neben seinem Amt kein weiteres besoldetes Amt und kein Gewerbe ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben. Seine Rechtsstellung wird im übrigen durch Vertrag geregelt.

(4) Der Datenschutzbeauftragte ist berechtigt und kann von der Mehrheit des Abgeordnetenhauses oder eines Ausschusses verpflichtet werden, vor dem Parlament oder dem betreffenden Ausschuß zu erscheinen und zu reden.

§ 23

Verschwiegenheitspflicht

Der Datenschutzbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Datenschutzbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Präsidenten des Abgeordnetenhauses weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen abgeben.

§ 24

Aufgaben und Befugnisse

(1) Der Datenschutzbeauftragte kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen. Zu diesem Zweck kann er Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er den Senat und einzelne Mitglieder des Senats sowie die übrigen Behörden und sonstigen öffentlichen Stellen in Fragen des Datenschutzes beraten.

(2) Ausgenommen von Absatz 1 sind die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Setzen Gerichte zur Erfüllung ihrer gesetzlichen Aufgaben automatische Datenverarbeitungsanlagen ein, so unterliegt unbeschadet der richterlichen Unabhängigkeit die Ordnungsmäßigkeit und Rechtmäßigkeit der Verfahren der Kontrolle des Datenschutzbeauftragten.

(3) Der Datenschutzbeauftragte beobachtet die Auswirkungen der automatischen Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der Behörden und sonstigen öffent-

lichen Stellen dahingehend, ob sie zu einer Beschränkung der Kontrollmöglichkeiten durch das Abgeordnetenhaus oder die Bezirksverordnetenversammlungen führen. Er kann Maßnahmen zum Schutz gegen derartige Auswirkungen anregen. Der Datenschutzbeauftragte ist über die Einführung neuer Automationsvorhaben im Bereich der Behörden und sonstigen öffentlichen Stellen zu informieren.

(4) Der Datenschutzbeauftragte arbeitet mit den Behörden und sonstigen öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, und mit den Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes zusammen. Er ist berechtigt, an andere Datenschutzbeauftragte und die Aufsichtsbehörden personenbezogene Daten zu übermitteln, soweit dies zur Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften erforderlich ist. Er ist ferner berechtigt, für diese Stellen auf ihr Ersuchen die Einhaltung datenschutzrechtlicher Vorschriften zu kontrollieren und in diesem Zusammenhang personenbezogene Daten zu erheben und sie an diese Stellen zu übermitteln.

(5) Der Datenschutzbeauftragte ist befugt, personenbezogene Daten, die ihm durch Beschwerden, Anfragen, Hinweise und Beratungsersuchen bekannt werden, zu verarbeiten, soweit dies zur Erfüllung seiner Aufgaben nach diesem Gesetz und dem Bundesdatenschutzgesetz erforderlich ist. Er darf im Rahmen von Kontrollmaßnahmen im Einzelfall personenbezogene Daten auch ohne Kenntnis des Betroffenen erheben, wenn nur auf diese Weise festgestellt werden kann, ob ein datenschutzrechtlicher Mangel besteht. Die nach den Sätzen 1 und 2 erhobenen und verarbeiteten Daten dürfen nicht zu anderen Zwecken weiterverarbeitet werden. Soweit der Datenschutzbeauftragte von seinem Strafantragsrecht nach § 32 Abs. 3 Gebrauch macht, ist er befugt, der Staatsanwaltschaft personenbezogene Daten zu übermitteln, soweit dies zur Durchführung des Ermittlungsverfahrens erforderlich ist.

§ 25

Dateienregister

(1) Der Datenschutzbeauftragte führt ein Register der Dateien, in denen personenbezogene Daten gespeichert werden, und der Geräte, mit denen diese Daten verarbeitet werden. Das Register kann von jedem eingesehen werden. Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, die von ihnen betriebenen Dateien und die verwendeten Geräte beim Datenschutzbeauftragten anzumelden. Dazu legen sie dem Datenschutzbeauftragten die Dateibesreibungen und Geräteverzeichnisse nach § 19 Abs. 2 und 4 vor. Die Dateien des Landesamtes für Verfassungsschutz, der Behörden der Staatsanwaltschaft und der Polizei, soweit diese nicht Ordnungsaufgaben wahrnimmt, sowie der Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern, können in einem besonderen Register geführt werden.

Anmerkungen:

Anmerkungen:

Diese Dateien werden auf Antrag der genannten Behörden nach Anhörung des Datenschutzbeauftragten bei Vorliegen eines besonderen öffentlichen Interesses an der Geheimhaltung der Dateien in dieses besondere Register aufgenommen. Dateien der Anstalten nach § 2 Abs. 2 werden im besonderen Register geführt. Satz 2 findet auf die besonderen Register keine Anwendung.

(2) Das Nähere regelt der Senat durch Rechtsverordnung.

§ 26

Beanstandungen

(1) Stellt der Datenschutzbeauftragte Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzvorschriften oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei Behörden und sonstigen öffentlichen Stellen der Hauptverwaltung gegenüber dem zuständigen Mitglied des Senats, im übrigen gegenüber dem Präsidenten des Abgeordnetenhauses oder dem Präsidenten des Rechnungshofs,
2. bei Behörden und sonstigen öffentlichen Stellen der Bezirksverwaltungen gegenüber den Bezirksamtern,
3. bei den landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen des Satzes 1 Nr. 2 und 3 unterrichtet der Datenschutzbeauftragte gleichzeitig auch das für die Aufsicht zuständige Mitglied des Senats.

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

(3) Mit der Beanstandung kann der Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die nach Absatz 1 Satz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Datenschutzbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 2 und 3 genannten Stellen leiten dem für die Aufsicht zuständigen Mitglied des Senats eine Abschrift ihrer Stellungnahme an den Datenschutzbeauftragten zu.

§ 27

Anrufung

Jedermann kann sich an den Datenschutzbeauftragten wenden, wenn er der Ansicht ist, daß bei der Verarbeitung personenbezogener Daten durch Behörden oder sonstige öffentliche Stellen gegen die Vorschriften dieses Gesetzes oder gegen andere Daten-

schutzvorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht. Dies gilt auch für Dienstkräfte der Behörden und sonstigen öffentlichen Stellen, ohne daß der Dienstweg einzuhalten ist.

§ 28

Unterstützung

(1) Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, den Datenschutzbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen sind dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme,
2. die in Nummer 1 genannten Unterlagen und Akten herauszugeben,
3. jederzeit Zutritt in alle Diensträume zu gewähren.

Satz 2 gilt für die in § 25 Abs. 1 Satz 5 genannten Behörden nicht, soweit das jeweils zuständige Mitglied des Senats im Einzelfall feststellt, daß die Einsicht in die Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Auf Antrag des Datenschutzbeauftragten hat die Senatsverwaltung dies im zuständigen Ausschuß des Abgeordnetenhauses in geheimer Sitzung zu begründen. Die Entscheidung des Ausschusses kann veröffentlicht werden.

(2) Berufs- und Amtsgeheimnisse entbinden nicht von der Unterstützungspflicht.

§ 29

Berichte und Gutachten

(1) Auf Anforderung des Abgeordnetenhauses oder des Senats hat der Datenschutzbeauftragte Gutachten zu erstellen und Berichte zu erstatten.

(2) Außerdem hat er dem Abgeordnetenhaus und dem Regierenden Bürgermeister jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Der Regierende Bürgermeister führt eine Stellungnahme des Senats zu dem Bericht herbei und legt diese regelmäßig innerhalb von drei Monaten nach Vorlage des Berichts dem Abgeordnetenhaus vor.

(3) Auf Ersuchen des Abgeordnetenhauses, des Petitionsausschusses des Abgeordnetenhauses oder des Senats hat der Datenschutzbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenkreis unmittelbar betreffen, nachzugehen. Der Datenschutzbeauftragte kann sich jederzeit an das Abgeordnetenhaus wenden.

Anmerkungen:

Anmerkungen:

Fünfter Abschnitt
Besonderer Datenschutz

§ 30

Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zwecke wissenschaftlicher Forschung dürfen datenverarbeitende Stellen personenbezogene Daten ohne Einwilligung des Betroffenen nur für bestimmte Forschungsarbeiten übermitteln,

1. soweit dessen schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden, oder
2. wenn 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.

Die Übermittlung bedarf der vorherigen Zustimmung der obersten Landesbehörde oder einer von dieser bestimmten Stelle; dies gilt nicht für die Anstalten nach 2 Abs. 2. Die Zustimmung muß den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Berliner Datenschutzbeauftragten mitzuteilen.

(2) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern, die Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist.

(3) Eine Verarbeitung der nach Absatz 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Absatz 1 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiter übermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Absätze 2 und 3 einzuhalten, und sich der Kontrolle des Berliner Datenschutzbeauftragten unterwirft.

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

- a) der Betroffene eingewilligt hat oder
- b) dieses für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(6) Unter den Voraussetzungen des Absatzes 1 darf die datenverarbeitende Stelle personenbezogene Daten ohne Einwilligung des Betroffenen selbst zum Zwecke wissenschaftlicher Forschung verarbeiten.

§ 31

Datenverarbeitung zu journalistisch-redaktionellen Zwecken

(1) Soweit der Sender Freies Berlin personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet, gelten nicht die §§ 9 bis 14 sowie die §§ 21 bis 29.

(2) Führt die journalistisch-redaktionelle Verarbeitung personenbezogener Daten zur Veröffentlichung von Gegendarstellungen der Betroffenen, so sind die Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Der Sender Freies Berlin bestellt einen Beauftragten für den Datenschutz, der die Vorschriften über den Datenschutz im journalistisch-redaktionellen Bereich frei von Weisungen überwacht. An ihn kann sich jedermann wenden, wenn er annimmt, bei der Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen Zwecken in seinen Rechten verletzt worden zu sein. Beanstandungen richtet der Beauftragte für den Datenschutz an den Intendanten und unterrichtet gleichzeitig den Rundfunkrat. Die Dienstaufsicht obliegt dem Verwaltungsrat.

§ 31 a

Fernmeß- und Fernwirkdienste

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmeßdienste) in Wohnungen oder Geschäftsräumen nur vornehmen oder mittels einer Übertragungseinrichtung in Wohnungen oder Geschäftsräumen andere Wirkungen nur auslösen (Fernwirkdienste), wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes der Dienste unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Der Betroffene kann seine Einwilligung jederzeit widerrufen. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Die Einrichtung von Fernmeß- und Fernwirkdiensten ist nur zulässig, wenn der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist, und wenn der Teilnehmer den Dienst jederzeit abschalten kann, soweit dies mit dem Vertragszweck vereinbar ist.

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

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

Anmerkungen:

Anmerkungen:

Sechster Abschnitt
Schlußvorschriften

§ 32

Straftaten

(1) Wer unbefugt personenbezogene Daten, die nicht offenkundig sind,

1. übermittelt oder verändert oder
2. abrufen oder sich aus in Behältnissen verschlossenen Dateien verschafft,

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

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

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt ist der Betroffene. Antragsberechtigt ist auch der Datenschutzbeauftragte. Der Datenschutzbeauftragte ist auch gegen den Willen des Betroffenen antragsberechtigt.

§ 33

Aufsichtsbehörde nach dem Bundesdatenschutzgesetz

(1) Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes ist der Berliner Datenschutzbeauftragte. Er untersteht insoweit der Rechtsaufsicht des Senats.

(2) Die Aufsichtsbehörde erhält von den Gewerbebeamten Durchschriften der An-, Um- bzw. Abmeldungen von Betrieben, die nach dem Kenntnisstand der Gewerbeämter der Meldepflicht des § 32 Abs. 1 des Bundesdatenschutzgesetzes unterfallen. Wenn der Aufsichtsbehörde im Rahmen ihrer rechtmäßigen Aufgabenerfüllung Tatsachen bekannt werden, die auf eine gewerberechtliche Unzuverlässigkeit hindeuten, kann sie diese Tatsachen den Gewerbebeamten mitteilen.

(3) Die Aufsichtsbehörde ist befugt, personenbezogene Daten, die ihr im Rahmen von Beschwerden und Anfragen bekannt werden, zu verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben nach dem Bundesdatenschutzgesetz erforderlich ist. Sie darf personenbezogene Daten im Rahmen von Kontrollmaßnahmen im Einzelfall auch ohne Kenntnis der Betroffenen erheben, wenn nur auf diese Weise festgestellt werden kann, ob ein datenschutzrechtlicher Mangel besteht. Die nach den Sätzen 1 und 2 verarbeiteten Daten dürfen nicht zu anderen Zwecken weiterverarbeitet werden.

§ 34

Besondere Regelungen

(1) aufgehoben.

(2) Abweichend von § 2 Abs. 1 gelten anstelle der §§ 9 bis 17 dieses Gesetzes die §§ 13, 28, 31, 33 bis 35, 39 und 44 des Bundesdatenschutzgesetzes, soweit die Datenverarbeitung frühere, bestehende oder künftige dienst- oder arbeitsrechtliche Rechtsverhältnisse betrifft. Die Vorschriften des Bundesdatenschutzgesetzes sind entsprechend auch auf die Verarbeitung in Akten anzuwenden.

(3) Abweichend von § 13 ist die Einwilligung des Betroffenen nicht erforderlich bei der Übermittlung personenbezogener Daten aus den Anzeigen Gewerbetreibender nach den §§ 14 und 55 c der Gewerbeordnung soweit die Übermittlung zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht.

(Abs. [3] ist durch §§ 11 Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften, vom 23. November 1994 [BGBl. S. 3475] bedeutungslos geworden – Anm. d. Red.)

(4) Für eine Übergangszeit bis zum 31. Januar 1993 dürfen Daten zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, wenn sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint.

§ 35

Änderung des Gesetzes
über das Verfahren der Berliner Verwaltung

Das Gesetz über das Verfahren der Berliner Verwaltung vom 8. Dezember 1976 (GVBl. S. 2735, 2898), zuletzt geändert durch Gesetz vom 24. April 1990 (GVBl. S. 877), wird wie folgt geändert:

1. § 1 Abs. 1 wird wie folgt gefaßt:

„(1) Für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden Berlins gilt das Verwaltungsverfahrensgesetz (VwVfG) vom 25. Mai 1976 (BGBl. I S. 1253/GVBl. S. 1173), geändert durch Gesetz vom 2. Juli 1976 (BGBl. I S. 1749/GVBl. S. 1620), soweit nicht in den §§ 2 bis 4 dieses Gesetzes etwas anderes bestimmt wird.“

Anmerkungen:

Anmerkungen:

2. Es wird folgender neuer §2a eingefügt:

„§2 a

Personenbezogene Daten,
Betriebs- und Geschäftsgeheimnisse

(1) Die Behörde darf Angaben über persönliche und sachliche Verhältnisse einer natürlichen Person und Betriebs- und Geschäftsgeheimnisse nicht unbefugt offenbaren. Sie unterliegt, soweit sie personenbezogene Daten verarbeitet, den Vorschriften des Berliner Datenschutzgesetzes.

(2) §26 Abs. 2 Satz 3 des Verwaltungsverfahrensgesetzes findet mit der Maßgabe Anwendung, daß auch eine Pflicht zur Angabe von personenbezogenen Daten oder von Betriebs- und Geschäftsgeheimnissen nur besteht, soweit sie durch Rechtsvorschrift besonders vorgesehen ist. Der Beteiligte kann die Auskunft auf solche Fragen, zu denen er durch Rechtsvorschrift verpflichtet ist, verweigern, wenn eine Beantwortung ihn selbst oder einen der in §383 Abs. 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

(3) Abweichend von §29 Abs. 2 des Verwaltungsverfahrensgesetzes ist die Behörde den Beteiligten zur Gestattung der Einsicht in die das Verfahren betreffenden Akten nach §29 Abs. 1 des Verwaltungsverfahrensgesetzes nicht verpflichtet, soweit eine Abwägung ergibt, daß die dort gewährten Rechte der Beteiligten hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten müssen; die wesentlichen Gründe für die Verweigerung der Akteneinsicht sind den Beteiligten im einzelnen mitzuteilen.“

§36

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt am Tage nach der Verkündung im Gesetz- und Verordnungsblatt für Berlin in Kraft.

(2) Gleichzeitig treten außer Kraft

1. das Gesetz über den Datenschutz in der Berliner Verwaltung (Berliner Datenschutzgesetz BlnDSG) vom 12. Juli 1978 (GVBl. S. 1317), zuletzt geändert durch Gesetz vom 30. Oktober 1984 (GVBl. S. 1541),
2. die Datenschutzveröffentlichungsordnung (BlnDsVeröffO) vom 27. Juli 1978 (GVBl. S. 1567).

(3) Die Senatsverwaltung für Inneres wird ermächtigt, das Berliner Datenschutzgesetz mit neuer fortlaufender Paragraphenfolge bekanntzumachen und dabei Unstimmigkeiten des Wortlauts zu beseitigen.

3. Informationsverarbeitungsgesetz

Gesetz über die Informationsverarbeitung bei der allgemeinen Verwaltungstätigkeit (Informationsverarbeitungsgesetz – IVG)

in der Fassung vom 9. Oktober 1992 (GVBl. S. 305)

§ 1

Anwendungsbereich

(1) Dieses Gesetz regelt die Verarbeitung personenbezogener Daten bei der manuellen und automatisierten allgemeinen Verwaltungstätigkeit, soweit hierfür keine besonderen gesetzlichen Vorschriften gelten oder im Hinblick auf das informationelle Selbstbestimmungsrecht erforderlich sind.

(2) Im Sinne dieses Gesetzes umfaßt allgemeine Verwaltungstätigkeit die Vorgangsverwaltung, die Dokumentation der Vorgänge und der Verfahrensbeteiligten, die Bürokommunikation sowie sonstige zur ordnungsgemäßen Erledigung der behördlichen Aufgaben erforderliche organisatorische Tätigkeiten, insbesondere den dafür notwendigen Schriftwechsel innerhalb der Verwaltung und nach außen sowie die Erstellung, Verwaltung oder Archivierung der im Rahmen des Geschäftsgangs notwendigen Aufzeichnungen. Als allgemeine Verwaltungstätigkeit gilt auch die Bearbeitung von Anträgen und Vorgängen, die keinem gesetzlich geregelten Sachgebiet zugeordnet werden können, ferner die Durchführung von Rechtsstreitigkeiten.

(3) Dieses Gesetz gilt für die Behörden und sonstigen öffentlichen Stellen des Landes Berlin, der landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, soweit diese nicht am Wettbewerb teilnehmen, sowie für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

§ 2

Datenschutz bei der allgemeinen Verwaltungstätigkeit

(1) Die in § 1 Abs. 3 genannten Stellen dürfen personenbezogene Daten bei der Wahrnehmung ihrer Aufgaben ohne Einwilligung des Betroffenen verarbeiten, soweit dies für die allgemeine Verwaltungstätigkeit erforderlich ist und schutzwürdige Belange des Betroffenen wegen der Art der Daten, wegen der Art der Verwendung oder wegen ihrer Offenkundigkeit nicht entgegenstehen.

Anmerkungen:

(2) Für Dateien mit diesen Daten sind Benachrichtigungen des Betroffenen, Dateibesreibungen und die Anmeldung der Dateien zum Dateienregister beim Berliner Datenschutzbeauftragten gemäß § 16 Abs. 2, § 19 Abs. 2 und § 25 des Berliner Datenschutzgesetzes in der Fassung vom 17. Dezember 1990 (GVBl. 1991 S. 16, 54), zuletzt geändert durch Gesetz vom 26. März 1992 (GVBl. S. 81), nicht erforderlich.

(3) Die datenverarbeitenden Stellen haben für die in Absatz 2 genannten Dateien in einer Kurzbeschreibung schriftlich festzulegen

1. die Bezeichnung der Datei und ihre Zweckbestimmung,
2. die Art der gespeicherten Daten und
3. den Kreis der Betroffenen.

(4) Automatisierte Verfahren der allgemeinen Verwaltungstätigkeit sind von Verfahren, in denen personenbezogene Daten auf Grund besonderer gesetzlicher Vorschriften verarbeitet werden, durch geeignete technische Maßnahmen zu trennen, soweit nicht die Verbindung am Arbeitsplatz erforderlich ist. Automatisierte Auswertungen von personenbezogenen Daten sind außer zu den Zwecken der allgemeinen Verwaltungstätigkeit nur zu Zwecken des Datenschutzes oder der Datensicherheit oder mit dem Einverständnis der Betroffenen im Einzelfall zulässig.

§ 3

Abgeordnetenhaus-Dokumentations- und Informationssystem

(1) Das Abgeordnetenhaus von Berlin richtet für das Parlament ein Dokumentations- und Informationssystem ein, aus dem auch die Berliner Verwaltung und die Öffentlichkeit Daten abrufen dürfen.

(2) Zur Veröffentlichung bestimmte Dokumente dürfen auch insoweit, als sie personenbezogene Daten enthalten, in dem Dokumentations- und Informationssystem bereitgestellt werden, wenn diese Daten Gegenstand öffentlicher Sitzungen des Abgeordnetenhauses oder seiner Gremien waren oder wenn schutzwürdige Belange Betroffener einer Veröffentlichung nicht entgegenstehen.

(3) Nicht zur Veröffentlichung bestimmte Dokumente sind durch geeignete technische Maßnahmen vom Dokumentations- und Informationssystem getrennt zu halten.

§ 4

Risikoanalyse

Vor der Entscheidung über den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens der allgemeinen Verwaltungstätigkeit ist zu prüfen, ob und in welchem Umfang mit der Nutzung der Informationstechnik Gefahren für die Rechte der Betroffenen oder für die Funktionsfähigkeit der Verwaltung verbunden sind. Automatisierte Verfahren dürfen nur eingesetzt

oder wesentlich geändert werden, soweit derartige Risiken durch technische oder organisatorische Maßnahmen wirksam beherrscht werden können. Die Entscheidung trifft der Leiter der die Informationstechnik einsetzenden Stelle. Er unterrichtet den Berliner Datenschutzbeauftragten über die Entscheidung.

§ 5

Inkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung im Gesetz- und Verordnungsblatt für Berlin in Kraft.