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 30. November 2007 (GVBl. S. 598)

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, gesperrt, 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.

(2) Betrifft die Datenverarbeitung frühere, bestehende oder künftige dienst- oder arbeitsrechtliche Rechtsverhältnisse, so gelten anstelle der §§ 9 bis 17 dieses Gesetzes § 28 Abs. 1 und 3 Nr. 1, §§ 31, 33 bis 35, 39 und 43 des Bundesdatenschutzgesetzes, soweit nichts anderes geregelt ist. Dies gilt auch für die Verarbeitung in Akten.

(3) Für öffentliche Stellen, die am Wettbewerb teilnehmen, gelten die §§ 3, 6, 6a, 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 43 des Bundesdatenschutzgesetzes.

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

(5) 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 Ge-

setz 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. Der Auftrag ist unter Festlegung des Gegenstandes und des Umfangs der Datenverarbeitung, der technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse schriftlich zu erteilen. Der Auftraggeber hat sich von der Einhaltung der Maßnahmen nach Satz 3 zu überzeugen.

(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 Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit unterwirft. Wird die Datenverarbeitung in einem anderen Bundesland oder in einem Mitgliedstaat der Europäischen Union durchgeführt, ist sicherzustellen, dass der Auftragnehmer einer Datenschutzkontrolle durch die jeweils zuständige Stelle unterliegt. Der Auftraggeber hat den Berliner Beauftragten für Datenschutz und Informationsfreiheit über die Beauftragung zu unterrichten.

§ 3a
Wartung

(1) Datenverarbeitungssysteme sind so zu gestalten, dass bei ihrer Wartung möglichst nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht sichergestellt ist, hat die datenverarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann. Dabei sind insbesondere folgende Anforderungen zu erfüllen: Es ist

1. sicherzustellen, dass nur dafür autorisiertes Personal die Wartung vornimmt,

2. sicherzustellen, dass jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgen kann,

3. zu verhindern, dass personenbezogene Daten im Rahmen der Wartung unbefugt entfernt oder übertragen werden,

4. sicherzustellen, dass alle Wartungsvorgänge während der Durchführung kontrolliert werden können,

5. sicherzustellen, dass alle Wartungsvorgänge nach der Durchführung nachvollzogen werden können,

6. zu verhindern, dass bei der Wartung Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden,

7. zu verhindern, dass bei der Wartung Datenverarbeitungsprogramme unbefugt verändert werden können, und

8. die Wartung so zu organisieren und zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Eine Wartung durch andere Stellen darf über die Anforderungen nach Absatz 1 hinaus nur auf Grund schriftlicher Vereinbarungen erfolgen. Darin sind folgende Regelungen zu treffen:

1. Art und Umfang der Wartung,

2. Abgrenzung der Rechte und Pflichten zwischen Auftraggeber und Auftragnehmer,

3. eine Protokollierungspflicht beim Auftraggeber und die Verpflichtung des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen und sich an dessen Weisungen zu halten,

4. die Daten dürfen ausschließlich für den Zweck der Wartung verwendet werden,

5. Sicherstellung, dass keine Datenübermittlung an andere Stellen durch den Auftragnehmer erfolgt,

6. Löschung der Daten nach Abschluss der Wartungsarbeiten,

7. die technische Verbindung muss vom Auftraggeber hergestellt werden, sofern dies nicht möglich ist, ist ein Rückrufverfahren verbindlich festzulegen,

8. Anwesenheit des Systemverwalters ist möglichst sicherzustellen,

9. Verschlüsselung von personenbezogenen Daten auf dem Übertragungsweg nach dem jeweiligen Stand der Technik und

10. für den Fall, dass ein Auftragnehmer außerhalb der Mitgliedstaaten der Europäischen Union aus tätig wird, sind stets die jeweiligen Regelungen des § 14 über die Übermittlung personenbezogener Daten an ausländische und internationale Stellen anzuwenden.

Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

(3) Ist bei Wartungsarbeiten nur ein Zugriff auf Daten in verschlüsselter, pseudonymisierter oder anonymisierter Form gegeben, so dass die mit der Wartung betraute Stelle Betroffene nicht reidentifizieren kann, so sind nur Maßnahmen nach Absatz 2 Satz 1 und 3 erforderlich. Ein Zugriff darf nur zweckgebunden erfolgen.

(4) Im Sinne dieses Gesetzes ist

a) Wartung die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie die Überprüfung und Reparatur oder der Austausch von Hardware,

b) Fernwartung die Wartung der Hard- und Software von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung personenbezogener Daten erfolgt, mittels Einrichtung zur Datenübertragung vorgenommen wird, und

c) Verschlüsselung das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann.

§ 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 abruft,

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. Empfänger jede Person oder Stelle, die Daten erhält,

3. 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 der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union Daten im Auftrag verarbeitet,

4. automatisierte Datenverarbeitung jede durch Einsatz eines gesteuerten technischen Verfahrens selbständig ablaufende Datenverarbeitung,

5. 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),

6. eine Akte jede sonstigen amtlichen oder dienstlichen Zwecken dienende Unterlage, soweit sie nicht Datei im Sinne von Nummer 5 ist; dazu zählen auch Bild- und Tonträger, nicht jedoch Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen,

7. Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

8. Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

9. mobiles personenbezogenes Speicher- und Verarbeitungsmedium ein Datenträger,

   a) der an den Betroffenen ausgegeben wird,

   b) auf dem personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

   c) bei dem der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

§ 5
Technische und organisatorische Maßnahmen

(1) Die Ausführungen der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Die Art und Weise der Maßnahmen hat für den angestrebten Schutzzweck angemessen zu sein und richtet sich nach dem jeweiligen Stand der Technik.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die geeignet sind 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. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),

5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit), und

6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(3) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Dazu gehört bei Verfahren, mit denen Daten verarbeitet werden, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder die zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden, eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung. Entsprechend der technischen Entwicklung ist die Ermittlung in angemessenen Abständen zu wiederholen. Soweit trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken verbleiben, die nicht durch Maßnahmen nach den Absätzen 1 und 2 oder eine Modifizierung der automatisierten Datenverarbeitung verhindert werden können, darf ein Verfahren nicht eingesetzt werden.

(4) Werden personenbezogene Daten nicht automatisiert verarbeitet, so findet Absatz 2 Nr. 1 bis 4 entsprechende Anwendung.

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

§ 5a
Datenvermeidung

Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

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 erlaubt 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 bis 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.

(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 des Betroffenen ist nur wirksam, wenn sie auf seiner freien Entscheidung beruht. Sie ist insbesondere unwirksam, wenn sie durch Androhung ungesetzlicher Nachteile oder durch fehlende Aufklärung bewirkt wurde. Soweit besondere Kategorien personenbezogener Daten nach § 6a Abs. 1 verarbeitet werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

(6) Die Einwilligung kann auch elektronisch erklärt werden. Es muss dabei sichergestellt werden, dass die Anforderungen zum Nachweis der Authentizität der Einwilligung jenen Anforderungen entsprechen, die für das zu Grunde liegende Verwaltungshandeln verlangt werden.

§ 6a
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Personenbezogene Daten im Sinne des Artikels 8 Abs. 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) – EG-Datenschutzrichtlinie – dürfen nur verarbeitet werden, wenn angemessene Garantien zum Schutze des Rechtes auf informationelle Selbstbestimmung bestehen und eine besondere Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt, dies erlaubt.

(2) Die Verarbeitung dieser Daten ist auch zulässig, wenn der Betroffene ausdrücklich eingewilligt hat oder die Verarbeitung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist und der Betroffene aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, seine Einwilligung zu geben.

(3) Die Absätze 1 und 2 finden keine Anwendung, wenn

1. Daten auf der Grundlage von § 2 Abs. 2 oder § 30 dieses Gesetzes verarbeitet werden oder

2. die Datenverarbeitung 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.

§ 7
Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft, Benachrichtigung und Einsichtnahme (§ 16),

2. Berichtigung, Sperrung, Löschung und Widerspruch (§ 17),

3. Schadenersatz und Unterlassung (§ 18),

4. Einsicht in Beschreibungen und Verzeichnisse (§ 19a),

5. Anrufung des Berliner Beauftragten für Datenschutz und Informationsfreiheit (§ 27).

Auf diese Rechte kann der Betroffene nicht wirksam verzichten.

§ 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. Diese Verpflichtung ist für Personen, die bei nicht öffentlichen Auftragnehmern öffentlicher Stellen dienstlichen Zugang zu personenbezogenen Daten haben, vertraglich sicherzustellen.

(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 und des § 6a Abs. 1 und 2 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 ohne Kenntnis des Betroffenen 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

1. eine der Voraussetzungen des § 6 Abs.1 oder des § 6a Abs. 1 oder 2 vorliegt,

2. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

3. 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.

Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten

Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, findet Satz 1 Nr. 2 und 3 keine Anwendung.

(3) Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen 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 Kontrollbefugnissen, der internen Revision, 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 § 11 Abs. 2 Satz 1 Nr. 1 bis 3 vorliegt. Werden die Daten von einer Behörde oder sonstigen öffentlichen Stelle 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 der Behörde oder sonstigen öffentlichen Stelle 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 Dritten 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) Für die Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union gilt § 12 Abs. 1 entsprechend.

(2) Die Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union ist nur zulässig, soweit die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaft oder einer internationalen Vereinbarung ausdrücklich geregelt ist und wenn ein angemessenes Datenschutzniveau gewährleistet ist. Die Angemessenheit des Datenschutzniveaus ist von der übermittelnden Stelle unter Berücksichtigung aller Umstände der beabsichtigten Datenübermittlung zu beurteilen, insbesondere nach der Art der Daten, ihrer Zweckbestimmung, der Dauer der geplanten Verarbeitung, dem Herkunfts- und dem Endbestimmungsland, den für den Empfänger geltenden Rechtsnormen sowie den für ihn geltenden Standesregeln und Sicherheitsmaßnahmen.

(3) Ist in den Fällen des Absatzes 2 kein angemessenes Datenschutzniveau gewährleistet, ist eine Übermittlung personenbezogener Daten zulässig, wenn

1. der Betroffene eingewilligt hat,

2. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist,

4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind, oder

5. für die Übermittlung oder eine Kategorie von Übermittlungen insbesondere durch eine vertragliche Vereinbarung ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte sichergestellt werden.

Die Stelle, an die die Daten übermittelt werden, ist auf die Zweckbindung nach § 11 Abs. 1 hinzuweisen.

(4) Die Senatsverwaltung für Inneres, der Berliner Beauftragte für Datenschutz und Informationsfreiheit und der behördliche Datenschutzbeauftragte sind über eine geplante Datenübermittlung nach den Absätzen 2 und 3 rechtzeitig zu unterrichten. Sie ist in der Dateibeschreibung nach § 19 Abs. 2 zu verzeichnen.

(5) Die Absätze 2 bis 4 finden keine Anwendung, soweit im Rahmen des internationalen Rechtshilfeverkehrs personenbezogene Daten übermittelt werden, die nicht automatisiert verarbeitet werden und auch nicht in Dateien gespeichert sind oder gespeichert werden sollen. In diesem Fall ist eine Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union zulässig, wenn

1. die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaften oder einer internationalen Vereinbarung ausdrücklich geregelt ist oder

2. für den Empfänger gleichwertige Datenschutzregelungen gelten und bei einer Übermittlung an öffentliche Stellen die Voraussetzungen der §§ 9 und 11 erfüllt sind.

§ 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. 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 offen stehen oder deren Veröffentlichung zulässig wäre.

(5) Die Absätze 1, 2 und 4 sind auf die Zulassung regelmäßiger automatisierter Datenübermittlungen entsprechend anzuwenden.

§ 15a
Verbot automatisierter Einzelentscheidungen

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine Entscheidung nach Satz 1 kann durch Gesetz zugelassen werden, wenn es die Wahrung der berechtigten Interessen des Betroffenen sicherstellt.

§ 16
Auskunft, Benachrichtigung und Einsichtnahme

(1) Werden personenbezogene Daten in einem automatisierten Verfahren oder 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,

4. den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

(2) Werden personenbezogene Daten automatisiert verarbeitet, so ist der Betroffene von dieser Tatsache schriftlich zu benachrichtigen. Die Benachrichtigung umfasst einen Hinweis auf die Dateibeschreibung nach § 19 Abs. 2. 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.

(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.

(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 Beauftragten für Datenschutz und Informationsfreiheit wenden kann. Die datenverarbeitende Stelle muss dem Berliner Beauftragten für Datenschutz und Informationsfreiheit die Gründe der Auskunfts- oder Einsichtsverweigerung darlegen.

§ 17
Berichtigung, Sperrung und Löschung von Daten, Widerspruchsrecht

(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 1 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.

(7) Wenn der Betroffene schriftlich Widerspruch gegen die Datenverarbeitung einlegt und begründet, dass der rechtmäßigen Verarbeitung seiner Daten ein schutzwürdiges besonderes persönliches Interesse entgegensteht, ist die Verarbeitung der Daten nur zulässig, wenn im Einzelfall das öffentliche Interesse an der Datenverarbeitung gegenüber dem persönlichen Interesse des Betroffenen überwiegt; dem Betroffenen ist das Ergebnis der Abwägung mit Begründung schriftlich mitzuteilen.

§ 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 verarbeiten 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) Sind an einer automatisierten Bearbeitung mehrere Stellen beteiligt und lässt sich die speichernde Stelle nicht feststellen, so haftet jede dieser Stellen.

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

§ 19
Durchführung des Datenschutzes und Dateibeschreibung

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

(2) Für automatisierte Verarbeitungen hat die datenverarbeitende Stelle schriftlich festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle,

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung,

3. Beschreibung der betroffenen Personengruppe und der diesbezüglichen Daten oder Datenkategorien,

4. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden,

5. Herkunft regelmäßig empfangener Daten,

6. zugriffsberechtigte Personen oder Personengruppen,

7. Fristen für die Sperrung und Löschung der Daten,

8. geplante Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union,

9. Betriebsart des Verfahrens, Art der Geräte, Stellen, bei denen sie aufgestellt sind, und das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung,

10. Beschreibung der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (§ 5 Abs. 3 Satz 1),

11. Ergebnisse der Vorabkontrollen (§ 19a Abs. 1 Satz 3 Nr. 1).

(3) Absatz 2 findet keine Anwendung auf Dateien, die bei automatisierter Verarbeitung ausschließlich aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden.

§ 19a
Behördlicher Datenschutzbeauftragter

(1) Die Behörden und sonstigen öffentlichen Stellen haben Datenschutzbeauftragte (behördliche Datenschutzbeauftragte) sowie jeweils einen Vertreter schriftlich zu bestellen. Für mehrere Behörden oder sonstige öffentliche Stellen kann ein gemeinsamer Datenschutzbeauftragter bestellt werden. Die behördlichen Datenschutzbeauftragten haben insbesondere

1. bei den mit besonderen Risiken für Rechte und Freiheiten von Betroffenen verbundenen Verarbeitungen vor Beginn der Verarbeitung eine Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach § 5 durchzuführen (Vorabkontrolle),

2. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen,

3. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenen besonderen Erfordernisse für den Datenschutz, vertraut zu machen und

4. die Behörde oder sonstige öffentliche Stelle bei der Sicherstellung des Datenschutzes zu unterstützen; sie unterstützen auch die Personalvertretungen bei der Sicherstellung des Datenschutzes, soweit bei diesen personenbezogene Daten verarbeitet werden.

Der behördliche Datenschutzbeauftragte führt die Beschreibungen und Verzeichnisse nach § 19. Diese können von jeder Person unentgeltlich eingesehen werden. Dies gilt nicht für die Angaben zu § 19 Abs. 2 Nr. 9 bis 11, soweit dadurch die Sicherheit des technischen Verfahrens beeinträchtigt wird. Dies gilt ferner nicht für Beschreibungen für Aufgaben des Verfassungsschutzes, der Gefahrenabwehr, der Strafverfolgung und der Steuerverwaltung, soweit die datenverarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt, sowie für öffentliche Stellen, die am Wettbewerb teilnehmen.

(2) Zum behördlichen Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird. Er muss in einem Dienst- oder Arbeitsverhältnis bei einer Behörde oder sonstigen öffentlichen Stelle des Landes Berlin oder einer landesunmittelbaren Körperschaft, Anstalt oder Stiftung

des öffentlichen Rechts stehen. Seine Bestellung kann gegen seinen Willen nur aus wichtigem Grund in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs widerrufen werden. Er kann sich in Angelegenheiten des Datenschutzes unmittelbar an den Leiter der jeweiligen Behörde oder sonstigen öffentlichen Stelle wenden und unterliegt in Datenschutzangelegenheiten keinen Weisungen. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Er ist zur Verschwiegenheit über die Identität Betroffener sowie über die Umstände, die Rückschlüsse auf Betroffene zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(3) Der behördliche Datenschutzbeauftragte ist befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Die jeweilige Behörde oder sonstige öffentliche Stelle hat den behördlichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Er ist über Vorhaben der automatisierten Verarbeitung rechtzeitig zu unterrichten.

(4) Der behördliche Datenschutzbeauftragte kann sich jederzeit an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden. In Zweifelsfällen der Vorabkontrolle ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit zu konsultieren.

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. 3 Satz 1 Nr. 3 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 Beauftragter für Datenschutz und Informationsfreiheit

§ 21
Bestellung und Entlassung

(1) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit wird vom Abgeordnetenhaus mit den Stimmen der Mehrheit seiner Mitglieder gewählt und vom Präsidenten des Abgeordnetenhauses ernannt. Er nimmt zugleich die Aufgaben des Beauftragten für Akteneinsicht nach § 18 Abs. 1 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das durch Artikel XXII des Gesetzes vom 16. Juli 2001 (GVBl. S. 260)

geändert worden ist, wahr und führt die Amts- und Funktionsbezeichnung "Berliner Beauftragter für Datenschutz und Informationsfreiheit" in männlicher oder in weiblicher Form.

(2) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragten für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis.

(2) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit 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. Er ist vor dem Erlass von den Datenschutz betreffenden Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften anzuhören.

§ 23
Verschwiegenheitspflicht

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekannt gewordenen 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit 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. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist bei der Vorabkontrolle nach § 5 Abs. 3 zu beteiligen, wenn sie den beabsichtigten Einsatz verwaltungsübergreifender Verfahren betrifft. Er hat darüber hinaus die Befugnisse, die den für Datenschutz zuständigen Aufsichts- und Kontrollbehörden durch internationale oder europäische Rechtsakte zugewiesen werden.

(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 Berliner Beauftragten für Datenschutz und Informationsfreiheit.

(3) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit beobachtet die Auswirkungen der automatischen Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der Behörden und sonstigen öffentlichen 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit ist über die Einführung neuer Automationsvorhaben und wesentliche Änderungen automatisierter Datenverarbeitungen im Bereich der Behörden und sonstigen öffentlichen Stellen zu informieren.

(4) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 diese Stellen 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; dies gilt auch, wenn sich eine nicht öffentliche Stelle durch Vertrag seiner Kontrolle unterworfen hat. Er leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe).

(5) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit 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

(aufgehoben)

§ 26
Beanstandungen

(1) Stellt der Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Rechnungshofes,

2. bei Behörden und sonstigen öffentlichen Stellen der Bezirksverwaltungen gegenüber den Bezirksämtern,

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 Berliner Beauftragte für Datenschutz und Informationsfreiheit gleichzeitig auch das für die Aufsicht zuständige Mitglied des Senats.

(2) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit 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 Berliner Beauftragten für Datenschutz und Informationsfreiheit 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 Berliner Beauftragten für Datenschutz und Informationsfreiheit zu.

§ 27
Anrufung

Jedermann kann sich an den Berliner Beauftragten für Datenschutz und Informationsfreiheit 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 Datenschutzvorschriften 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 Berliner Beauftragten für Datenschutz und Informationsfreiheit 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 und Kopien von Unterlagen, von automatisierten Dateien, von deren Verfahren und von organisatorischen Regelungen zur Mitnahme zur Verfügung zu stellen,

3. jederzeit Zutritt in alle Diensträume und Zugriff auf elektronische Einrichtungen zu gewähren.

Satz 2 gilt für die in § 19a Abs. 1 Satz 7 genannten Aufgaben 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 Berliner Beauftragten für Datenschutz und Informationsfreiheit 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit Gutachten zu erstellen und Berichte zu erstatten.

(2) Er hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Der Senat legt dem Abgeordnetenhaus regelmäßig innerhalb von drei Monaten nach Vorlage des Berichts eine Stellungnahme zu dem Bericht vor.

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

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 öffentlichen Stellen nach § 2 Abs. 3. Die Zustimmung muss den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Berliner Beauftragten für Datenschutz und Informationsfreiheit 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 weiterübermittelt 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 Beauftragten für Datenschutz und Informationsfreiheit 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 durch den Sender Freies Berlin

(1) Soweit der Sender Freies Berlin personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet, gelten anstelle dieses Gesetzes § 22a des Berliner Pressegesetzes vom 15. Juni 1965 (GVBl. S. 744), das zuletzt durch Artikel VI des Gesetzes vom 30. Juli 2001 (GVBl. S. 305) geändert worden ist, und § 41 Abs. 2 und 3 des Bundesdatenschutzgesetzes entsprechend.

(2) 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 oder literarischen 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.

§ 31a
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 des Dienstes 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.

§ 31b
Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit der Einsatz der Videoüberwachung zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die datenverarbeitende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(3a) Für Daten, die in öffentlich zugänglichen Räumen des öffentlichen Personennahverkehrs nach Absatz 1 erhoben oder nach Absatz 3 Satz 1 gespeichert werden, gilt anstelle von Absatz 3 Satz 2, dass

1. sie für einen anderen Zweck nur verarbeitet werden dürfen, soweit dies zur Abwehr oder für die Verfolgung von Straftaten erforderlich ist, und

2. für diesen Zweck ihre Übermittlung ausschließlich an den Polizeipräsidenten in Berlin und an die Strafverfolgungsbehörden zulässig ist.

Aufzeichnungen, deren Speicherung weder für die Abwehr noch für die Verfolgung von Straftaten erforderlich ist, sind spätestens nach 24 Stunden zu löschen. Dies ist durch ein mit dem Polizeipräsidenten in Berlin abzustimmendes Sicherheitskonzept zu gewährleisten.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung, die Identität der verarbeitenden Stelle sowie über die Zweckbestimmung der Verarbeitung zu benachrichtigen. Der Betroffene ist auch über die

Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen. Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. eine Abwägung ergibt, dass das Benachrichtigungsrecht des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung aus zwingenden Gründen zurücktreten muss,

2. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

3. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder

4. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist.

Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 3 oder 4 abgesehen wird.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 31c
Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,

2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,

3. darüber, wie er seine Rechte nach den §§ 16 und 17 ausüben kann, und

4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

Sechster Abschnitt

Schlussvorschriften

§ 32

Straftaten

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

1. übermittelt oder verändert oder

2. abruft 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 Berliner Beauftragte für Datenschutz und Informationsfreiheit. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist auch gegen den Willen des Betroffenen antragsberechtigt.

§ 33
Aufsichtsbehörde nach dem Bundesdatenschutzgesetz

(1) Aufsichtsbehörde nach dem Bundesdatenschutzgesetz für die Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Er untersteht insoweit der Rechtsaufsicht des Senats, die entsprechend der §§ 10 bis 13 des Allgemeinen Zuständigkeitsgesetzes ausgeübt wird.

(2) Die Aufsichtsbehörde erhält von den Gewerbeämtern Durchschriften der An-, Um- bzw. Abmeldungen von Betrieben, die nach dem Kenntnisstand der Gewerbeämter der Meldepflicht des § 4d 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 Gewerbeämtern 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

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

§ 35
Änderung des Gesetzes

über das Verfahren der Berliner Verwaltung

(überholt)

§ 36
Inkrafttreten, Außerkrafttreten

(vom Abdruck wird abgesehen)