VIS BE

Gesamtes Gesetz

Amtliche Abkürzung:	BlnDSG		
Neugefasst durch Bek. vom:	17.12.1990	**Quelle:**	
Gültig ab:	10.11.1990	**Fundstelle:**	GVBl. 1991, 16, 54
Dokumenttyp:	Gesetz	**Gliederungs-Nr:**	205-1

Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG) in der Fassung vom 17. Dezember 1990

Zum 16.04.2018 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: letzte berücksichtigte Änderung: § 26 geändert durch Artikel 23 des Gesetzes vom 02.02.2018 (GVBl. S. 160)

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 Absatz 2 Nummer 2, §§ 31 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, 6 a, 9 bis 17,

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) 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 großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

(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.

§ 5 a
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 oder elektronisch 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 § 6 a 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

(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 § 6 a 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 § 6 a 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

(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 Gemeinschaft 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.

Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

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

(7) Für die Einrichtung gemeinsamer Verfahren und automatisierter Abrufverfahren für verschiedene Zwecke innerhalb einer öffentlichen Stelle gelten die Absätze 1 bis 5 entsprechend.

(8) Die Absätze 1 bis 7 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

(9) Die Absätze 1, 4, 6 und 8 sind auf die Zulassung regelmäßiger automatisierter Datenübermittlungen entsprechend anzuwenden.

§ 15 a
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 oder elektronisch 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

(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.

§ 18a
Informationspflicht bei unrechtmäßiger Kenntniserlangung von Dritten

(1) Wird einer datenverarbeitenden Stelle bekannt, dass bei ihr gespeicherte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, so hat sie dies unverzüglich dem Betroffenen und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit mitzuteilen.

(2) Die Benachrichtigung des Betroffenen nach Absatz 1 darf nur solange aufgeschoben werden, wie die verantwortliche Stelle zunächst angemessene Maßnahmen zur Sicherung der Daten ergreifen muss. Ergreift sie diese Maßnahmen nicht unverzüglich, so duldet die Benachrichtigung des Betroffenen keinen Aufschub. Satz 1 gilt entsprechend, soweit eine unverzügliche Benachrichtigung des Betroffenen die Strafverfolgung gefährden würde. Die Betroffenen sind über die Art der unrechtmäßigen Kenntniserlangung und über Maßnahmen zur Minderung möglicher nachteiliger Folgen zu unterrichten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, tritt an ihre Stelle eine angemessene Information der Öffentlichkeit.

§ 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 oder elektronisch 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,

nur aus wichtigem Grund in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs widerrufen werden. Die Kündigung des Arbeitsverhältnisses des nach Absatz 1 bestellten behördlichen Datenschutzbeauftragten ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die Behörden und sonstigen öffentlichen Stellen zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach Abberufung als behördlicher Datenschutzbeauftragter ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die Behörden und sonstigen öffentlichen Stellen zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt sind. Der behördliche Datenschutzbeauftragte 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 davon nicht 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.

(5) Zum Erwerb und zur Erhaltung der zur Erfüllung seiner Aufgaben erforderlichen Fachkunde haben die Behörden und sonstigen öffentlichen Stellen dem behördlichen Datenschutzbeauftragten die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

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 Absatz 1 Satz 1 Nummer 2 oder 3 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

und einzelne Mitglieder des Senats sowie die übrigen Behörden und sonstigen öffentlichen Stellen in Fragen des Datenschutzes beraten. Er ist vor dem Erlass von Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften anzuhören, wenn sie die Verarbeitung personenbezogener Daten betreffen. 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
- 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

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

(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 48 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 oder elektronisch 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.

§ 31 c
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,

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 Dritte ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht.

§ 35
Änderung des Gesetzes über das Verfahren der Berliner Verwaltung

(Änderungsanweisungen)

§ 35a
Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 des Bundesdatenschutzgesetzes in der bis zum 31. August 2009 geltenden Fassung weiter anzuwenden für Zwecke der Werbung bis zum 31. August 2012.

§ 36
Inkrafttreten, Außerkrafttreten

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

(2) *(Aufhebungsanweisungen)*

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

© juris GmbH