Amtsblatt für Brandenburg

Gemeinsames Ministerialblatt für das Land Brandenburg

9. Jahrgang	Potsdam, den 3. Februar 1998	Nummer 4

Inhalt Seite

Ministerium des Innern

Verwaltungsvorschriften des Ministeriums des Innern zur Durchführung des Brandenburgischen Datenschutzgesetzes (VV zum BbgDSG) 94

Zusammenschluß der Gemeinden Schönborn, Lindena, Gruhno und Schadewitz zu einer neuen Gemeinde Schönborn 112

Ministerium der Finanzen

Auslandsumzugskostenverordnung - AUV - Durchführungsvorschriften des Auswärtigen Amts und des Bundesministeriums des Innern zur AUV - 112

Ministerium für Ernährung, Landwirtschaft und Forsten

Richtlinie des Ministeriums für Ernährung, Landwirtschaft und Forsten über die Gewährung von Zuwendungen aus den Mitteln der Walderhaltungsabgabe und ihre Verwendung zum Zwecke der Erhaltung des Waldes 112

Ministerium für Stadtentwicklung, Wohnen und Verkehr

Erlaß des Ministeriums für Stadtentwicklung, Wohnen und Verkehr zur Förderung der behindertengerechten Anpassung von Mietwohnungen (Wohnraumanpassungserlaß) 114

Beilage: Amtlicher Anzeiger Nr. 4/1998

Verwaltungsvorschriften des Ministeriums des Innern zur Durchführung des Brandenburgischen Datenschutzgesetzes (VV zum BbgDSG)

Vom 17. Dezember 1997

Artikel 11 Abs. 1 Satz 1 der Verfassung des Landes Brandenburg gewährleistet, daß jeder Bürger selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann (Recht auf informationelle Selbstbestimmung). Das Recht auf informationelle Selbstbestimmung kann im überwiegenden Allgemeininteresse durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden. Die öffentliche Verwaltung benötigt im Interesse des Bürgers Angaben über persönliche Verhältnisse. Um den Datenverkehr zwischen den Bürgern und der Verwaltung und innerhalb der Verwaltung zu regeln, wurde das Brandenburgische Datenschutzgesetz (BbgDSG) vom 20. Januar 1992 (GVBl. I S. 2) geschaffen, wobei das Gesetz insoweit verdrängt wird, als bereichsspezifische Regelungen des Bundes oder des Landes Brandenburg den Umgang mit personenbezogenen Daten betreffen (§ 2 Abs. 3 Satz 2 BbgDSG). Zwischenzeitlich ist das Gesetz zweimal geändert worden. Die Neubekanntmachung des Gesetzes vom 23. Mai 1996 (GVBl. I S. 185), geändert durch das Brandenburgische Statistikgesetz (BbgStatG) vom 11. Oktober 1996 (GVBl. I S. 294), berücksichtigt das am 23. Januar 1996 in Kraft getretene Änderungsgesetz. Die Datenverarbeitung erfolgt zunehmend mittels moderner Informationstechnik, die durch die rasche Entwicklung ständig vervollkommnet wird, so daß eine immer schnellere Verarbeitung oder ein schnellerer Zugriff auf die personenbezogenen Daten möglich wird. Das Datenschutzgesetz verpflichtet die öffentliche Verwaltung, die unten näher erläuterten Maßnahmen zu treffen, um der Gefahr einer Verletzung des informationellen Selbstbestimmungsrechts entgegenzuwirken.

1. Begriffserläuterungen

1.1 **Behörde** ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt (§ 1 Abs. 2 des Verwaltungsverfahrensgesetzes für das Land Brandenburg (VwVfGBbg)), wobei die organisatorische Selbständigkeit der Behörde am eigenverantwortlichen Auftreten nach außen zu erkennen ist. Sonstige öffentliche Stellen sind nach außen eigenverantwortlich handelnde Stellen, die keine Behördeneigenschaft besitzen. Vereinigungen juristischer Personen des öffentlichen Rechts sind ungeachtet ihrer Rechtsform öffentliche Stellen, Vereinigungen öffentlicher Stellen des privaten Rechts jedoch nur, wenn sie Aufgaben der öffentlichen Verwaltung erfüllen. Soweit kommunale Gebietskörperschaften Eigengesellschaften (rechtlich selbständige Unternehmen in zivilrechtlichen Formen wie Aktiengesellschaften, Gesellschaften mit beschränkter Haftung) errichten oder an privatrechtlich organisierten wirtschaftlichen Unternehmen beteiligt sind, sind für solche Unternehmen die Vorschriften des Bundesdatenschutzgesetzes bezüglich der Datenverarbeitung durch nicht-öffentliche Stellen anzuwenden. Nehmen nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr (beliehene Unternehmen), sind auch diese Stellen öffentliche Stellen, wenn sie im Rahmen der Beleihung tätig werden (§ 2 Abs. 1 Satz 3 BbgDSG). Stellen nach § 2 Abs. 2 Satz 1 BbgDSG sind Eigenbetriebe und öffentliche Einrichtungen nach § 103 der Gemeindeordnung (GO) vom 15. Oktober 1993 (GVBl. I S. 398), die entsprechend den Vorschriften der Verordnung über die Eigenbetriebe (EigV) vom 27. März 1995 (GVBl. II S. 314) geführt werden, sowie der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen. Eigenbetriebe sind wirtschaftliche Unternehmen kommunaler Gebietskörperschaften ohne eigene Rechtspersönlichkeit, die nach § 95 Abs. 1 Nr. 1 GO als Sondervermögen der Gemeinde zu führen sind. Sie können nach § 101 Abs. 3 Nr. 1 GO sowohl unter den Voraussetzungen des § 100 GO als auch zur Erfüllung der in § 101 Abs. 2 GO genannten Aufgaben gegründet werden. Die den Eigenbetrieben nach § 2 Abs. 2 Satz 1 Nr. 2 BbgDSG gleichstehenden öffentlichen Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden, haben derzeit nach der Systematik der Brandenburgischen Gemeindeordnung keine Bedeutung, da § 103 Abs. 1 GO hinsichtlich der Freiheit der Wahl der Rechtsform für die wirtschaftliche Betätigung der Gemeinden über den abschließenden Katalog des § 101 Abs. 3 GO hinaus keinen neuen Sachverhalt schafft. Zu den juristischen Personen des öffentlichen Rechts, die der Aufsicht des Landes unterliegen und am Wettbewerb teilnehmen, zählen u. a. Sparkassen.

1.2 **Personenbezogene Daten** sind Einzelangaben, die eine natürliche Person (Betroffener) bestimmen oder bestimmbar machen [z. B. Name, Personalnummer (§ 3 Abs. 1 BbgDSG)]. Als Einzelangaben gelten weiterhin Daten, die einen in der Person des Betroffenen liegenden oder auf den Betroffenen bezogenen Sachverhalt beschreiben (z. B. Adresse, Geburtsdatum, Einkommen) sowie jegliche andere Angaben zu einer Person, die dieser zugeordnet werden können.

1.3 **Datenverarbeitende Stellen** sind die Stellen, die Daten selbst verarbeiten oder durch andere verarbeiten lassen (§ 3 Abs. 4 Nr. 1 BbgDSG). Datenverarbeitende Stellen sind die Behörden und die von ihnen getragenen sonstigen öffentlichen Stellen. Nachgeordnete Bereiche einer Behörde sind Teil der datenverarbeitenden Stelle, wenn sie nicht organisatorisch selbständig sind. Unter datenverarbeitenden Stellen sind auch solche Stellen zu verstehen, die selbst keine Daten speichern, sondern nur über ein Sichtgerät nutzen. Im Fall der Auftragsdatenverarbeitung gilt der Auftraggeber als datenverarbeitende Stelle.

1.4 Eine **Datei** ist eine Sammlung personenbezogener Daten, die automatisiert oder nicht-automatisiert vorgehalten werden kann (§ 3 Abs. 4 Nr. 3 BbgDSG). Eine **automatisierte Datei** ist ein elektronisch gespeicherter Datenbestand, in dem die Daten mittels automatisierter Verfahren verarbeitet werden können. Dazu zählen auch Bild- und Tonaufzeichnungen in digitalisierter Form. Unter einer **nicht-automatisierten Datei** ist eine Datensammlung zu

verstehen, die ohne Einsatz der Automation nach bestimmten Merkmalen geordnet und ausgewertet werden kann (z. B. Karteikartensammlung).

1.5 **Akten** sind sonstige Unterlagen, die dienstlichen Zwecken dienen und nicht Datei sind. Notizen und Vorentwürfe, die nicht Bestandteil eines Vorgangs werden sollen und alsbald vernichtet werden, werden von diesem Begriff nicht erfaßt (§ 3 Abs. 4 Nr. 4 BbgDSG).

1.6 **Datenschutzverantwortliche** sind diejenigen Mitarbeiterinnen und Mitarbeiter einer Behörde, die die jeweilige öffentliche Stelle bei der Umsetzung der Datenschutzvorschriften unterstützen und beraten sowie innerhalb der öffentlichen Stelle auf die Einhaltung der datenschutzrechtlichen Vorschriften im Interesse der Gewährleistung des Grundrechts auf informationelle Selbstbestimmung achten. Die Aufgaben der Datenschutzverantwortlichen werden unter Nummern 2.11 und 2.12 näher bezeichnet.

2. Zu § 7 BbgDSG (Sicherstellung des Datenschutzes)

2.1 § 7 BbgDSG regelt die Fragen der eigenverantwortlichen Durchführung des Datenschutzes in der Landesverwaltung, der Kommunalverwaltung und den der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen. Die Vorschrift wendet sich an die in § 2 Abs. 1 BbgDSG genannten öffentlichen Stellen und verpflichtet sie, für ihren Bereich die Ausführung aller Datenschutzvorschriften sicherzustellen.

2.2 Die in § 2 Abs. 1 Satz 1 BbgDSG genannten öffentlichen Stellen haben insbesondere dafür zu sorgen, daß die in Datenschutzvorschriften enthaltenen Verbote eingehalten werden, Datenschutzpflichten erfüllt und die notwendigen Datensicherungsmaßnahmen getroffen und eingehalten werden. Außerdem müssen die Aufgaben und Verantwortlichkeiten für den Datenschutz nach § 10 BbgDSG im Rahmen der Geschäftsverteilung klargestellt werden. Eine wichtige Aufgabe besteht in der Gewährleistung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden. Dazu gehört z. B. das Sicherstellen, daß Programme nur zu vorgesehenen Zwecken eingesetzt werden. Die Nutzer sollen in ihren Fachanwendungen nur die Daten abrufen können, die sie für ihre Tätigkeit benötigen. Des weiteren zählt dazu, daß das entsprechende Personal, das mit der Verarbeitung personenbezogener Daten betraut werden soll, ausgewählt und zur fachgerechten Anwendung der Datenverarbeitungsprogramme befähigt wird.

2.3 Die Art und Weise der Ausführung der Datenschutzvorschriften bleibt den Normadressaten überlassen, um damit den Besonderheiten der verschiedenen Verwaltungszweige Rechnung zu tragen.

2.4 Zur Sicherstellung der Art und Weise der Ausführung der Datenschutzvorschriften in bezug auf einzelne Verfahren können durch die obersten Landesbehörden weitergehende Verwaltungsvorschriften erlassen werden. Vor dem Erlaß dieser Verwaltungsvorschriften ist der Landesbeauftragte für den Datenschutz (LfD) zu hören. Der LfD ist auch vor dem Erlaß von Rechtsvorschriften (Gesetze, Verordnungen, Satzungen), die die Verarbeitung personenbezogener Daten betreffen, zu hören. Dienstanweisungen, welche lediglich den internen Dienstverkehr regeln, gehören nicht hierzu.

2.5 Bevor ein automatisiertes Verfahren zur Verarbeitung personenbezogener Daten zum ersten Mal zum Einsatz gebracht wird, bedarf es einer schriftlichen Freigabe hinsichtlich der in der Dateibeschreibung (§ 8 Abs. 1 BbgDSG) festzulegenden Angaben (Freigabeverfahren). Mit der Verpflichtung zur Durchführung eines Freigabeverfahrens und der damit verbundenen Überprüfung eines Verfahrens soll erreicht werden, daß eine Auswahl aus den automatisierten Verfahren erfolgt und nur solche Verfahren zum Einsatz kommen, die auch die datenschutzrechtlichen Bedingungen erfüllen. Die Datenschutzverantwortlichen sollen bereits zu Beginn der Programmentwicklung beteiligt werden.

2.6 Im Bereich der Landesverwaltung erklärt die oberste Landesbehörde, die für die dem automatisierten Verfahren zugrunde liegende Rechtsmaterie zuständig ist, die Freigabe und in allen anderen Fällen die jeweils zuständige datenverarbeitende Stelle.

2.7 Im Rahmen der Freigabe ist zu überprüfen, ob die vorgesehene Verarbeitung der Daten datenschutzrechtlich zulässig ist (§ 4 BbgDSG), ob das Programm den vorgesehenen Zweck erfüllen kann und welche geeigneten Sicherungsmaßnahmen (§ 10 BbgDSG) im Hinblick auf die einzusetzende Hard- und Software getroffen werden müssen. Für das Freigabeverfahren kann das Formblatt „Dateibeschreibung gemäß § 8 BbgDSG“ (Anlage 1) verwendet werden. Das Formblatt enthält eine Beschreibung der automatisiert geführten Datei, in der personenbezogene Daten gespeichert sind (siehe unten Nummern 3.1 bis 3.3).

2.8 Ein Freigabeverfahren ist auch dann durchzuführen, wenn in einem bereits freigegebenen Verfahren wesentliche Änderungen durchgeführt werden. Solche Änderungen können z. B. Programmänderungen oder -erweiterungen sein, bei denen neue oder modifizierte Dateien entstehen.

2.9 Um Mehraufwand zu vermeiden, sollten gleichartige Verfahren zunächst von einer Stelle als Musterlösung erprobt werden. Für die Behörden und Einrichtungen der Landesverwaltung gilt: Verfahren für gleichartige Querschnittsaufgaben (z. B. Personalverwaltung, Reisekosten) oder Verwaltungsfunktionen (z. B. Schriftgutverwaltung, -archivierung) sind gemäß Nummer 3.5.3 der IT-Richtlinien Brandenburg vom 25. Juli 1991 (ABl. S. 392) ressortübergreifend abzustimmen. Dies erfolgt über das jeweils zuständige Ministerium im „Interministeriellen Ausschuß für Informationstechnik (IMA-IT)“.

2.10 Über Planungen zum Aufbau automatisierter Informationssysteme mit personenbezogenem Inhalt ist der LfD zu einem Zeitpunkt zu informieren (§ 23 Abs. 2 Satz 4 BbgDSG), zu dem noch eventuelle Bedenken berücksichtigt werden können.

2.11 Staatlichen und kommunalen Stellen wird empfohlen, eine Person, die für den Datenschutz verantwortlich ist, zu benennen (Datenschutzverantwortlicher). Diese Person berät und unterstützt die öffentlichen Stellen in allen Angelegenheiten, die für den Datenschutz bedeutsam sein können, und achtet darüber hinaus darauf, daß innerhalb der öffentlichen Stelle die datenschutzrechtlichen Vorschriften eingehalten werden. Ihr können insbesondere folgende Aufgaben übertragen werden:

a) Sammlung der Dateibeschreibungen (§ 8 Abs. 1 BbgDSG),
b) Erstellung einer Dateiübersicht,
c) Beteiligung bei der Führung des Geräteverzeichnisses (§ 8 Abs. 4 BbgDSG),
d) Beratung der Behörde bei Datensicherheitsmaßnahmen (§ 10 BbgDSG),
e) Anhörung bei der Erarbeitung behördeninterner Dienstanweisungen,
f) Mitwirkung bei der Freigabe von automatisierten Verfahren,
g) Mitwirkung bei der Vorbereitung und dem Abschluß von Verträgen nach § 11 und § 11 a BbgDSG.

Bei Maßnahmen nach Buchstabe f soll die Person, die für den Datenschutz zuständig ist, von Beginn der Programmentwicklung an beteiligt werden.

2.12 Mit der Funktion der oder des Datenschutzverantwortlichen soll eine Person betraut werden, die die erforderliche Sach- und Fachkunde besitzt. Die erforderliche Fachkunde ist dann gegeben, wenn die oder der Datenschutzverantwortliche über die notwendigen Kenntnisse des Datenschutzrechts verfügt, die besonderen Risiken der automatisierten Datenverarbeitung einzuschätzen vermag und in der Lage ist, die ihm obliegenden Aufgaben der Beratung und Schulung in Datenschutzfragen wahrzunehmen. Die notwendigen Kenntnisse müssen nicht bereits zum Zeitpunkt der Benennung umfassend vorhanden sein, sondern können unverzüglich nach der Benennung im Selbststudium oder durch den Besuch von Fortbildungsveranstaltungen erworben werden. Solange die Person, die für den Datenschutz verantwortlich ist, nicht über die ausreichenden Kenntnisse verfügt, kann im Rahmen der Bestellung vorgesehen werden, daß sie sich (vorübergehend) der Kenntnisse anderer Personen bedient. Soweit im Einzelfall fachspezifische Fragen nur in Zusammenarbeit mit anderen Personen gelöst werden können, bleibt es den Datenschutzverantwortlichen unbenommen, sich der Kenntnisse Dritter zu bedienen. Mitarbeiterinnen und Mitarbeiter des Personalreferates sowie Bedienstete, die zu selbständigen Entscheidungen in Personalangelegenheiten der Dienststelle befugt sind, scheiden für die Wahrnehmung dieser Funktion aus. Ebenso darf die Person, die das System betreut, nicht dieselbe Person sein, die für den Datenschutz verantwortlich ist.

2.13 Eine öffentliche Stelle, die einen Datenschutzverantwortlichen benennt, hat diesen schriftlich zu bestellen und die ihm obliegenden Aufgaben genau zu bezeichnen. Im Interesse einer raschen und effektiven Umsetzung datenschutzrechtlicher Vorschriften hat die öffentliche Stelle den Datenschutzverantwortlichen bei der Erfüllung seiner Aufgaben zu unterstützen und rechtzeitig über alle Maßnahmen, die für den Datenschutz bedeutsam sein könnten, zu unterrichten. Weiterhin hat die öffentliche Stelle durch organisatorische Maßnahmen sicherzustellen, daß der Datenschutzverantwortliche seine Vorschläge und Bedenken innerhalb der Leitung der öffentlichen Stelle vortragen kann.

2.14 Datenschutzverantwortliche sind bei der Erfüllung ihrer Aufgaben an Weisungen nicht gebunden. Sie dürfen wegen der Erfüllung ihrer Aufgaben nicht benachteiligt werden.

3. Zu § 8 BbgDSG (Dateibeschreibung)

3.1 Dateibeschreibungen sind für automatisiert geführte Dateien, die personenbezogene Daten beinhalten, anzufertigen. Bei der Anfertigung einer Dateibeschreibung sind die Verordnung zur Dateibeschreibung (DBeschrV) vom 4. September 1996 (GVBl. II S. 695) und die vom LfD gegebenen Hinweise zum Ausfüllen der Formulare zum Dateienregister (Anlage 2) zu beachten.

3.2 Zur Erstellung einer Dateibeschreibung verpflichtet sind die in § 2 Abs. 1 und 2 BbgDSG genannten öffentlichen Stellen, die selbst personenbezogene Daten in Dateien speichern oder in ihrem Auftrag speichern lassen. Eine Ausnahme von der Pflicht, eine Dateibeschreibung zu erstellen, besteht für die datenverarbeitende Stelle dann, wenn sie keinen Einfluß auf die Programme hat, weil die Programme und Daten durch eine übergeordnete Stelle zentral betreut werden. In diesem Fall sind die Aufgaben der datenverarbeitenden Stelle durch die übergeordnete Stelle wahrzunehmen. Bei der Verarbeitung personenbezogener Daten im Auftrag besteht für den Auftragnehmer keine unmittelbare Pflicht zur Erstellung der Dateibeschreibung, in der Praxis wäre es von Vorteil, wenn der Auftragnehmer den Auftraggeber hierbei unterstützt.

3.3 Die Dateibeschreibung sollte von den Mitarbeitern, die mit dieser Datei arbeiten, unter Mitwirkung des Verantwortlichen für den Datenschutz zusammengestellt werden. Die Dateibeschreibungen werden in einer Dateiübersicht zusammengefaßt, die beim Datenschutzverantwortlichen geführt wird. Sie dient der Behörde zur Eigenkontrolle. Dem LfD ist sie auf Verlangen vorzulegen (§ 26 Abs. 1 Nr. 1 BbgDSG).

3.4 Die unter Nummern 3.1 bis 3.3 aufgeführte Pflicht, eine Dateibeschreibung zu erstellen, findet bei nicht-automatisierten Dateien, aus denen keine Daten an Dritte übermit-

telt werden, und bei automatisierten Dateien (z. B. Zwischen- und Hilfsdateien), die nur vorübergehend vorgehalten werden, keine Anwendung, da der damit verbundene Verwaltungsaufwand in keinem angemessenen Verhältnis zum Nutzen für den Schutz des Persönlichkeitsrechts stehen würde. Für den Begriff „vorübergehend" gibt es keine feste zeitliche Eingrenzung. Ein Vorhalten der Datei bis zu drei Monaten steht mit dem Gesetz noch in Einklang. Dazu gehören z. B. die Adreßdateien, die zum Erstellen von Serienbriefen verwendet und nur vorübergehend gespeichert werden.

3.5 Die mit Hilfe von Textverarbeitungssystemen erstellten Unterlagen unterliegen nur dann einer Pflicht zur Erstellung einer Dateibeschreibung, wenn über übliche Suchbefehle hinaus eine gezielte personenbezogene Auswertung (z. B. bei Vorhandensein entsprechender Auswertungsprogramme) nach bestimmten Merkmalen möglich ist.

3.6 Schriftstücke aus einfachen Schreibautomaten, soweit eine personenbezogene Auswertung nicht ermöglicht wird, gelten nicht als Dateien.

3.7 Die datenverarbeitenden Stellen sind außerdem verpflichtet, ein Geräteverzeichnis (Anlage 1 Blatt 6) zu erstellen. Darin werden alle Geräte geführt, auf denen personenbezogene Daten automatisiert verarbeitet werden. Nicht aufzuführen sind solche Geräte, mit denen eine personenbezogene Auswertung nicht möglich ist (einfache Schreibautomaten, Bildschirmschreibmaschinen). Weitere Hinweise des LfD zum Ausfüllen der Formulare zum Geräteverzeichnis sind in der Anlage 3 aufgeführt.

4. Zu § 9 BbgDSG (Automatisiertes Abrufverfahren und regelmäßige Datenübermittlung)

4.1 Der Einrichtung von automatisierten Verfahren zur Direktabfrage von personenbezogenen Daten aus Datenbeständen als Informationsaustausch zwischen Behörden und sonstigen öffentlichen Stellen kommt unter den Aspekten des Datenschutzes und der Datensicherung besondere Bedeutung zu. Die abrufende Stelle erhält durch den Anschluß die Möglichkeit, über den gesamten Datenbestand der datenverarbeitenden Stelle zu verfügen. Daher ist die Einrichtung automatisierter Abrufverfahren nur aufgrund bundes- oder landesrechtlicher Regelungen (Gesetze, Verordnungen) zulässig. Entsprechend der Verordnungsermächtigung in § 9 Abs. 2 Satz 1 BbgDSG können die Ministerinnen und Minister für ihren Geschäftsbereich die Einrichtung von automatisierten Abrufverfahren durch Rechtsverordnung zulassen. Vor der Einrichtung ist eine Prüfung vorzunehmen, ob dies unter Beachtung der Rechte der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

4.2 Die Behörden im Geschäftsbereich eines Ministeriums, die im Online-Verfahren Daten untereinander übermitteln wollen, müssen gegenüber dem Fachressort anregen, daß eine entsprechende Verordnung erlassen wird. Dazu sind eine Begründung sowie die Darstellung der vorgesehenen Datensicherungsmaßnahmen einzureichen. Des weiteren sind die Datenempfänger, die Datenart und der Zweck des Abrufes festzulegen. Der LfD ist gemäß 2.4 über den Erlaß einer entsprechenden Verordnung und die Einrichtung eines automatisierten Abrufverfahrens zu unterrichten.

4.3 Sofern innerhalb einer öffentlichen Stelle automatisierte Verfahren zur Weitergabe von Daten im Sinne von § 14 Abs. 5 BbgDSG eingerichtet werden, gilt Nummer 4.2 Satz 2 und 3 entsprechend.

4.4 Für private Stellen dürfen keine Daten, die in der öffentlichen Verwaltung gespeichert sind, für den Abruf im Online-Verfahren bereitgehalten werden. Hiervon ausgenommen sind Auskünfte an Betroffene und die Fälle der Nummern 4.5 und 4.6.

4.5 Für Datenbestände, die für jedermann zugänglich sind oder für eine Veröffentlichung freigegeben sind, treffen die Regelungen von 4.1 bis 4.4 nicht zu.

4.6 Sind Daten mit schriftlicher Einwilligung des Betroffenen zum Zwecke der Übermittlung im automatisierten Abrufverfahren gespeichert, bedarf die Einrichtung eines automatisierten Abrufverfahrens keiner darüber hinausgehender Rechtsgrundlage (z. B. nach § 9 Abs. 1 BbgDSG). Für die Erteilung der Einwilligung ist § 4 Abs. 2 Satz 2 und 3 BbgDSG zu beachten. Eine Unterrichtung des LfD über derartige Online-Verfahren ist nicht vorgesehen.

4.7 Die in den vorangehenden Absätzen getroffenen Regelungen finden auf die Zulassung sonstiger regelmäßiger Datenübermittlungen entsprechend Anwendung. Die Regelungen von 4.3 gelten auch für die Datenweitergabe im Sinne des § 14 Abs. 5 BbgDSG.

4.8 Die an einem Abrufverfahren beteiligten Stellen haben die nach § 10 BbgDSG erforderlichen Maßnahmen zu treffen.

5. Zu § 10 BbgDSG (Technische und organisatorische Maßnahmen)

5.1 Die sich aus § 10 Abs. 1 Satz 1 BbgDSG ergebende Verpflichtung zur Durchführung von Datensicherungsmaßnahmen gilt für die automatisierte und nicht-automatisierte Datenverarbeitung (also z. B. auch für manuelle Karteien und Akten - vgl. Nummer 1.4).

5.2 Es gilt dabei der Grundsatz der Verhältnismäßigkeit. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Die Verhältnismäßigkeit von Sicherungsmaßnahmen sollte aus einer Risikoanalyse abgeleitet werden. Alle auf ein Verfahren bezogenen Maßnahmen sind in ihrer Gesamtheit zu betrachten. Die Summe der zu treffenden Maßnahmen muß die notwendige Sicherheit gewährleisten. Im Rahmen der Verhältnismäßigkeitsprüfung ist auch die Sensibilität der zu schützenden Daten zu berücksichtigen. Je höher die Sensibilität, um so höher

muß die Wertigkeit einer Datensicherungsmaßnahme sein.

5.3 Für automatisierte Verfahren führt § 10 Abs. 2 BbgDSG zehn typische Bereiche auf, in denen Maßnahmen zur Datensicherung durchzusetzen sind. In der Anlage 2 sind Beispiele für die entsprechenden Sicherungsmaßnahmen für diese Bereiche enthalten. Weitere Informationen über technisch-organisatorische Maßnahmen können Unterlagen entnommen werden, die u. a. vom Bundesamt für Sicherheit in der Informationstechnik, vom Ministerium des Innern (MI) oder vom LfD herausgegeben werden.

5.4 In der öffentlichen Verwaltung ist es unerläßlich, personenbezogene Daten vorzuhalten. Der Einsatz moderner Informationstechnik ist zur Absicherung einer schnellen Verarbeitung der Daten notwendig. In den Behörden werden meist Arbeitsplatzcomputer zur Erfüllung der Aufgaben genutzt, die mit geeigneten Maßnahmen gesichert werden müssen. Die Anlage 4 zur Verwaltungsvorschrift enthält Empfehlungen, die beim Umgang mit Arbeitsplatzcomputern zu beachten sind.

5.5 Eingehende Schreiben an Stellen, die besonders sensible Daten verarbeiten (z. B. Beihilfestellen, Personalstellen, ärztlicher Dienst, Jugendhilfestellen) sind ungeöffnet an die Adressaten weiterzuleiten. Sensible Daten sind auch innerhalb einer Behörde im verschlossenen Umschlag zu transportieren.

5.6 Für nicht-automatisierte Dateien (z. B. für Karteien) und für Akten sind gemäß § 10 Abs. 3 BbgDSG geeignete Sicherheitsmaßnahmen zu ergreifen. Möglichkeiten, einen unbefugten Zugriff auf nicht-automatisierte Dateien und Akten bei der Bearbeitung, dem Transport und der Aufbewahrung zu verhindern, sind beispielsweise:

a) Abschließen der Tür beim Verlassen von Amtsräumen,
b) Einschließen von Akten, Verschließen von Karteikästen bei Abwesenheit,
c) Festlegen von Personen oder Personengruppen, die berechtigt sind, auf Akten und Karteien zuzugreifen,
d) Versiegeln von Akten, insbesondere Personalakten beim Versand,
e) bei internem Postversand im verschlossenen Umschlag, sonst als Einschreiben mit Rückschein oder als Wertpaket,
f) Regelungen für die behördeneigene Poststelle und
g) Regelungen für die Vernichtung von Akten und Karteien.

5.7 Soweit Vorentwürfe und Notizen nicht Bestandteil eines Vorgangs werden und personenbezogene Daten enthalten, ist eine ordnungsgemäße Vernichtung z. B. mittels eines Aktenvernichters, der den Anforderungen gemäß DIN-Norm 32757 entsprechen sollte, zu gewährleisten.

6. Zu § 11 BbgDSG (Verarbeitung personenbezogener Daten im Auftrag)

6.1 „Datenverarbeitung im Auftrag“ durch eine öffentliche Stelle liegt nur dann vor, wenn die öffentliche Stelle als Auftraggeber einem Auftragnehmer unselbständige Teile aus der Datenverarbeitungsaufgabe überträgt, die von ihrer Art her eine Aufgabe des Auftraggebers selbst ist. Dies ist z. B. dann der Fall, wenn der Auftragnehmer nur die Berechnung von Vergütungen der Mitarbeiter der Behörde vornimmt, nachdem ihm der Auftraggeber die für die Berechnung erforderlichen Werte und die persönlichen Daten derjenigen mitgeteilt hat, die Vergütungen erhalten werden. Keine „Datenverarbeitung im Auftrag“ liegt vor, wenn dem Auftragnehmer eine oder mehrere vollständige Aufgaben aus dem Aufgabenbereich des Auftraggebers übertragen werden; in diesem Fall spricht man von Funktionsübertragung. Hiervon sind die Fälle zu unterscheiden, in welchen die öffentliche Stelle z. B. einen Werkvertrag oder einen Kauf- oder Dienstvertrag mit einem Vertragspartner abschließt, um den Vertragspartner zur Erbringung einer Leistung zu veranlassen, die nicht im Aufgabenbereich der öffentlichen Stelle liegt, z. B. eine neue Software zu entwickeln oder einen Rechner zu kaufen.

6.2 Bei der Datenverarbeitung im Auftrag wie auch bei der Funktionsübertragung oder im Rahmen eines Werk- oder Dienstvertrages können personenbezogene Daten verarbeitet werden. Bei der „Verarbeitung personenbezogener Daten im Auftrag“ ist die Verarbeitung personenbezogener Daten der Hauptgegenstand des Vertrages, mittels dessen der Auftraggeber den Auftragnehmer mit der vertraglichen Tätigkeit betraut; der Auftraggeber, die öffentliche Stelle, bleibt für die ordnungsgemäße Datenverarbeitung und für die Einhaltung aller damit verbundenen Vorschriften verantwortlich. Aus dem Gesetzestext ergeben sich klare Vorgaben für die Pflichten des Auftraggebers bei der Vergabe von Aufgaben der Datenverarbeitung im Auftrag. In den Fällen der Funktionsübertragung und immer dann, wenn der Vertragspartner bei der Vertragserfüllung Leistungen aus dem eigenen Bereich erbringt, ist die ausführende Stelle selbst für die Einhaltung der Datenschutzvorschriften verantwortlich.

6.3 Der Gesetzgeber hat erhöhte Anforderungen an die Rahmenbedingungen für die Datenverarbeitung im Auftrag gestellt, wenn der Auftragnehmer keine öffentliche, sondern eine nicht-öffentliche Stelle ist: In diesen Fällen ist die Zustimmung (Erlaubnis oder Genehmigung) der zuständigen obersten Landesbehörde oder des Ministers des Innern erforderlich. § 11 Abs. 3 und 4 BbgDSG enthält weitere Regelungen, die bei der Beauftragung von „privaten“ (d. h. nicht-öffentlichen) Stellen und von öffentlichen Stellen des Bundes oder anderer Länder zu beachten sind.

6.4 In § 11 Abs. 2 BbgDSG werden bestimmte Behörden aufgezählt, für die die Vorgaben des Zweiten Abschnittes des BbgDSG - hierdurch wird die Zuständigkeit des LfD vorgegeben - und die Vorschriften über das Datengeheimnis (§ 6) sowie die organisatorisch-technischen Maßnahmen (§ 10) auch ohne die ausdrückliche Verpflichtung innerhalb des Auftragsverhältnisses gelten.

6.5 Im ersten Halbsatz von § 11 Abs. 3 BbgDSG sind besondere Vorschriften für solche Auftragnehmer vorgesehen, für die „die Vorschriften dieses Gesetzes ... keine Anwendung finden“: Es handelt sich dabei um nicht-öffentliche Stellen, da für diese das Bundesdatenschutzgesetz (BDSG) und nicht das BbgDSG Geltung hat, und um öffentliche Stellen eines anderen Bundeslandes oder des Bundes. Mit diesen Stellen ist zu vereinbaren, daß sie die Vorschriften des BbgDSG einhalten und daß sich die auftragnehmende Stelle, sofern sie ihren Sitz im Land Brandenburg hat, der Kontrolle durch den LfD unterwirft. Damit werden die (strengeren) Vorschriften, die für öffentliche Stellen gelten, für diese Auftragnehmer verbindlich vorgeschrieben, und die ursprünglich vorliegende Zuständigkeit (§ 38 BDSG) - in Brandenburg das MI - wird durch die Datenschutzkontrolle des LfD wahrgenommen.

6.6 Sollte die nicht-öffentliche Stelle oder eine öffentliche Stelle des Bundes oder eines anderen Landes die Datenverarbeitung im Auftrag „außerhalb des Geltungsbereichs dieses Gesetzes“ vornehmen, muß die „für den Ort der Auftragsdurchführung zuständige“ Kontrollbehörde über die vorgesehene Datenverarbeitung im Auftrag hierüber unterrichtet werden. Außerdem hat die öffentliche Stelle als Auftraggeber sowohl den LfD als auch das MI als die im Land Brandenburg zuständige Aufsichtsbehörde über die beabsichtigte Datenverarbeitung im Auftrag zu unterrichten. Bei einer Datenverarbeitung im Auftrag, die eine brandenburgische öffentliche Stelle z. B. an eine nicht-öffentliche Stelle außerhalb von Brandenburg vergibt, besteht daher eine doppelte Informationspflicht: einerseits ist die am Ort der Datenverarbeitung zuständige Kontrollbehörde und andererseits in Brandenburg sowohl der LfD als auch das MI von der Auftragsvergabe in Kenntnis zu setzen.

6.7 In den Fällen der Datenverarbeitung im Auftrag, die im Ausland durchgeführt werden sollen, ist § 11 BbgDSG nicht einschlägig. Dies ergibt sich unmittelbar aus § 3 Abs. 4 BbgDSG. Stellen oder Personen, die im Ausland für öffentliche Stellen des Landes Daten im Auftrag verarbeiten, sind „Dritte” im Sinne des Gesetzes, so daß für die Weitergabe von Daten an diese Einrichtungen § 17 BbgDSG zur Anwendung kommt.

6.8 Die Auftragsvergabe an die nicht-öffentliche Stelle und die Annahme des Auftrags sind Teile eines Vertrages. Der Vertrag ist aus Gründen der Präzisierung des Auftrages und zum sicheren Nachweis der Einzelheiten der Beauftragung in schriftlicher Form abzuschließen (§ 11 Abs. 1 Satz 4 BbgDSG). Dies ergibt sich auch schon aus der Formulierung „der Auftraggeber ist verpflichtet, sicherzustellen“, und gilt, da die Vorschrift im Brandenburgischen Datenschutzgesetz verankert ist, zumindest für alle Vorgaben, die den Datenschutz betreffen.

6.9 In § 11 Abs. 4 BbgDSG ist festgelegt, daß die vertraglichen Pflichten in bezug auf den Datenschutz in einem möglichen Unterauftragsverhältnis nicht geringer sein dürfen als in dem Hauptauftragsverhältnis.

7. Zu § 11 a (Wartung und Fernwartung)

7.1 „Wartung” im engeren Sinne betrifft die Überprüfung und gegebenenfalls die Reparatur sowie die Neuinstallation von Software; der Austausch oder die Reparatur von Hardware ist ebenfalls der „Wartung” zuzurechnen. Die „Fernwartung” betrifft die Wartung der Software oder der Hardware, die von einem Ort aus vorgenommen wird, der nicht zum Organisationsbereich derjenigen öffentlichen Stelle gehört, bei der die Verarbeitung personenbezogener Daten vorgenommen wird. Da die „Fernwartung” begrifflich nur eine besondere Form der Wartung ist, sind unter dem Wort „Wartung” im folgenden sowohl „Wartung” als auch „Fernwartung” zu verstehen, es sei denn, eine der beiden Formen der Wartung werden ausdrücklich als solche benannt. Es kommt nicht darauf an, ob die Wartung oder Fernwartung durch eine öffentliche oder durch eine nicht-öffentliche Stelle vorgenommen wird.

7.2 Die meisten Hinweise, die im Zusammenhang mit Wartung zu beachten sind, betreffen die Fernwartung, da durch Fernwartung und anläßlich von Fernwartung eine Vielzahl von Beeinträchtigungen und Gefährdungen der Integrität und Vertraulichkeit personenbezogener Daten - und damit des Rechts auf informationelle Selbstbestimmung der betroffenen Personen - erfolgen kann: Es besteht in besonders starkem Maße die Gefahr, daß auf personenbezogene Daten zugegriffen wird. Der Datenschutz ist bei der Fernwartung nur unter großen Anstrengungen zu gewährleisten, da Fernwartung in aller Regel unter Nutzung der allgemeinen und öffentlich zugänglichen Netze erfolgt.

7.3 Sofern in einer datenverarbeitenden Stelle keine personenbezogenen Daten verarbeitet werden oder sofern sich bei Wartungsmaßnahmen keine personenbezogenen Daten in dem zu wartenden System befinden, sind aus der Sicht des Datenschutzes keine besonderen Sicherungsmaßnahmen bei der Wartung oder Fernwartung erforderlich. So kann der Datenschutz z. B. dadurch gewährleistet werden, daß vor einem Wartungsvorgang die personenbezogenen Daten aus dem zu wartenden System (i. d. Regel vorübergehend) entfernt werden. Auch bei Wartung unter Verwendung von Test-Programmen muß sichergestellt sein, daß nicht z. B. anläßlich von Wartung personenbezogene Daten offenbart werden oder von Dritten wahrgenommen werden können.

7.4 Wartungsmaßnahmen sind immer auf die im Sinne des Datenschutzes jeweils am wenigsten „gefährliche” Weise vorzunehmen. In jedem einzelnen Fall der Wartung ist sicherzustellen, daß der Datenschutz gewahrt wird. Daher sind neben den im Gesetz genannten technischen und organisatorischen Maßnahmen „vor Ort” regelmäßig zusätzlich auch vertragliche Festlegungen zur Einhaltung des Datenschutzes erforderlich. Das gilt auch in den Fällen von § 11 a Abs. 1, obwohl „schriftliche Vereinbarungen” allein in § 11 a Abs. 2 genannt werden, andernfalls könnte nicht gewährleistet werden, daß eine unbefugte Offenbarung personenbezogener Daten ausgeschlossen wird. Die vertraglichen Festlegungen der Fernwartung

sollen in einem gesonderten Vertrag vorgenommen werden. Soweit Stellen außerhalb des öffentlichen Bereiches mit Wartungsarbeiten betraut werden, müssen die mit den Wartungsarbeiten betrauten Personen zuvor schriftlich auf die Wahrung des Datengeheimnisses verpflichtet worden sein.

7.5 Zusätzlich zu den in § 10 BbgDSG festgelegten Maßgaben sollen zur Gewährleistung des Datenschutzes in den Fällen der Fernwartung je nach Art der zu schützenden personenbezogenen Daten und je nach Anwendungserfordernis die folgenden Maßnahmen - gegebenenfalls nebeneinander - durchgeführt werden:

a) Einschränkung der Zugriffsrechte und Zugriffsmöglichkeiten in bezug auf die Person, die die Fernwartung durchführt, soweit dies zur Sicherstellung des Datenschutzes erforderlich ist, daher ist z. B. darauf zu achten, daß im System unterschiedliche Nutzerprofile angelegt sind,
b) zusätzlich zur Anlegung unterschiedlicher Nutzerprofile sind die Einschränkungen durch vertragliche Vorgaben sicherzustellen; dies betrifft vorrangig die Anforderung, daß die Fernwartung von Anwenderprogrammen nur unter einer Kennung vorgenommen werden kann, die keine Systemverwalterprivilegien einschließt,
c) nach Möglichkeit die Verschlüsselung aller personenbezogener Daten, die dem Zugriff des Wartungspersonals nicht entzogen werden können,
d) „Identifikation" und „Authentisierung" des Personals, das die Fernwartung vornimmt, d. h., die Person, die die Fernwartung vornehmen soll, muß vor dem Wartungsvorgang vorab festgelegt werden; die fernwartende Person muß nachweisen, daß sie die vorab zur Fernwartung bestimmte Person tatsächlich ist,
e) Nutzung von automatisierten Rückrufverfahren beim Aufbau der (z. B. telefonischen) Verbindung zwischen der fernwartenden Stelle und der Stelle, an der die Wartung vorgenommen wird, oder die Zwischenschaltung eines Verfahrens, das mindestens den gleichen Sicherheitsstandard wie das Rückrufverfahren gewährleisten kann,
f) Geheimhaltung der jeweiligen Fernwartungs-Einwahlnummer der einzelnen zu wartenden Stellen (d. h. der Nummer des Eingabepunktes für die Fernwartung),
g) revisionssichere Protokollierung sämtlicher Aktivitäten bei der zu wartenden Stelle, solange die Verbindung zwischen wartender und zu wartender Stelle aufrechterhalten wird, und deren Verwahrung über einen angemessenen Zeitraum,
h) ständige Anwesenheit des Systemverwalters am Ort der Wartung während der Wartung oder Fernwartung und Sicherstellen der Möglichkeit, die Fernwartungsverbindung durch den örtlich dazu bestellten Systemverwalter unterbrechen zu lassen, sobald kritische Aktivitäten des Wartungspersonals bemerkt werden,
i) die Zulässigkeit für das Einspielen von Änderungen in das Betriebssystem ist durch vertragliche Regelungen so zu gestalten, daß derartige Vorgänge nur durch Maßnahmen vor Ort (d. h. durch Wartung), nicht jedoch durch Fernwartung zulässig sind; dies gilt nicht, wenn die Wartung durch eine andere öffentliche Stelle vorgenommen wird,
j) vertraglich ist sicherzustellen, daß personenbezogene Daten, die beabsichtigt oder unbeabsichtigt durch Wartung oder Fernwartung oder anläßlich derartiger Wartungsmaßnahmen an einen Ort außerhalb der zu wartenden Stelle gelangt sind, ausschließlich für Zwecke dieser Wartung verwendet werden dürfen und anschließend unverzüglich, spätestens aber nach Beendigung der Wartungsarbeiten, zu löschen sind.

7.6 Die vom LfD gegebenen Hinweise zum Ausfüllen der Formulare der Dateibeschreibung nach § 8 (Anlage 2) sind zu beachten.

8. Inkrafttreten/Außerkrafttreten

Die Verwaltungsvorschrift tritt am Tage der Bekanntmachung in Kraft. Gleichzeitig treten die Vorläufigen Verwaltungsvorschriften zur Durchführung des Brandenburgischen Datenschutzgesetzes vom 24. Januar 1995 (ABl. S. 134) außer Kraft.

Anlage 1

Ort, Datum

. . . . . .
Datenverarbeitende Stelle mit Anschrift

Dateibeschreibung gemäß § 8 BbgDSG

1. Bezeichnung der Datei

. . . . . .

❑ erstmaliges Anlegen

❑ Änderung einer Datei . . . . . .
(Es sind nur die eingetretenen Änderungen aufzuführen.)

❑ Löschung einer Datei . . . . . .
(In diesem Fall sind keine weiteren Angaben erforderlich.)

2. Zweckbestimmung der Datei

. . . . . .

3. Betroffener Personenkreis
(Falls möglich, sollte zusätzlich die Anzahl der betroffenen Personen - Schätzung - angegeben werden.)

. . . . . .

4. Datenverarbeitung im Auftrag (§ 11 BbgDSG)
(Hier wird gefragt, ob die Daten selbst oder durch einen Dritten verarbeitet werden. Die Dateibeschreibung ist nur vom Auftraggeber zu erstellen.)

❑ nein ❑ ja

Auftragnehmer mit Anschrift

Auftragnehmer ist eine

❑ öffentliche Stelle, auf die das BbgDSG Anwendung findet

❑ öffentliche Stelle, auf die das BbgDSG keine Anwendung findet (Bund, andere Bundesländer)

❑ nicht-öffentliche Stelle
Zustimmung der obersten Landesbehörde nach § 11 Abs. 1 BbgDSG liegt vor vom _____

5. Art der gespeicherten Daten			**6. bei regelmäßig empfangenen Daten deren Herkunft**	**7. bei regelmäßig zu übermittelnden Daten deren Empfänger**	**8. Rechtsgrundlage/n der Verarbeitung**	**9. Fristen für die Sperrung/Löschung der Daten**
Lfd. Nr.			(jeweils mit lfd. Nr/n aus Spalte 1)			
1	Familienname	❑				
2	Vornamen	❑				
3	Geburtsname	❑				
4	Geburtsdatum	❑				
5	Geburtsort	❑				
6	Anschrift	❑				
	weitere Daten					
8						
9						
10						
.						
.						
.						

Können über Schlüsselwörter Verbindungen zu anderen Dateien hergestellt werden ? ❑ ja ❑ nein

10. Technische und organisatorische Maßnahmen gemäß § 10 BbgDSG

10.1 Kurzbeschreibung der technischen und organisatorischen Maßnahmen gemäß § 10 Abs. 2 BbgDSG:

Zugangskontrolle	
Datenträgerkontrolle	
Speicherkontrolle	
Benutzerkontrolle	
Zugriffskontrolle	
Übermittlungskontrolle	
Eingabekontrolle	
Auftragskontrolle (Bitte insbesondere angeben, welche Maßnahmen und Vereinbarungen gem. § 11 Abs. 1 BbgDSG getroffen worden sind)	

Transportkontrolle	
Organisationskontrolle	

10.2 Ist einer Organisationseinheit die Überprüfung von Art und Umfang der getroffenen Datensicherungsmaßnahmen übertragen?

❑ ja ❑ nein

. . . . . .

10.3 Ist einer Organisationseinheit die Kontrolle der Einhaltung der zur Datensicherung bestehenden Vorschriften und Anweisungen übertragen?

❑ ja ❑ nein

. . . . . .

10.4 Gibt es eine Dienstanweisung für die Datensicherung?

❑ ja ❑ nein

. . . . . .

10.5 Existiert zu der Datei eine Paralleldatei mit fiktiven Daten zu Schulungs-, Test- und Servicezwecken?

❑ ja ❑ nein

---

11. Beschreibung des automatisierten Verfahrens

. . . . . .

. . . . . .

(Kurzbeschreibung)

a) Betriebsart des Verfahrens:

❑ Stapel-(Batch)Betrieb

❑ Dialog-Betrieb

❑ . . . . . .

b) Art der Geräte

❑ Großrechner (Host)

❑ Arbeitsplatzrechner/Mehrplatzsystem

❑ Arbeitsplatzrechner/Einplatzsystem

❑ . . . . . .

c) Stellen, bei denen die Geräte aufgestellt sind:

d) Verfahren (auch bei auftragsweiser Datenverarbeitung) zur

. . . . . .

Übermittlung

❑ Datenträger ❑ Magnetbänder ❑ Disketten ❑ Eingabebelege ❑ Ausdrucke

❑ Datenübertragung über Leitungen (Art, Typ, Prozedur, priv./öffentl. Netz)

. . . . . .

. . . . . .

Sperrung*)

. . . . . .

Löschung*)**)

. . . . . .

Auskunftserteilung*)

. . . . . .

*) soweit ein besonderes Verfahren vorgesehen ist
**) ggf. auch Termine für die Prüfung der Löschungsvoraussetzungen

Ort, Datum

. . . . . .
Datenverarbeitende Stelle mit Anschrift

Geräteverzeichnis gemäß § 8 BbgDSG

(Für jede Rechner-Zentraleinheit ist ein getrenntes Formular anzuwenden)

Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden:

1. Rechner, Zentraleinheit

Typ (bitte ankreuzen) Arbeitsplatzcomputer ❑ Mehrplatzsystem ❑ (auch Netzserver) Großrechner ❑

Hersteller:

Betriebssystem:

Kapazität des Arbeitsspeichers:

2. Peripherie des Rechners

Anzahl angeschlossener Terminals ❑ Drucker ❑ sonstige Ein-/Ausgabegeräte ❑

3. Vernetzung des Rechners

3.1 Lokales Netz

Typ:

Netz-Betriebssystem:

3.2 Einrichtungen zur Datenfernverarbeitung und -übertragung
Für jede Einrichtung bitte angeben:

Art	Typ	Prozedur	Postdienst	Empfänger

4. Programm zur Verarbeitung personenbezogener Daten

Name:

Hersteller:

verwendete
Standardsoftware:

Anlage 2

Hinweise zum Ausfüllen der Formulare zur Dateibeschreibung

Zu 1. Bezeichnung der Datei

In dieses Feld ist der physische oder logische Dateiname (Bezug auf Inhalt) oder - falls nicht anders möglich - der Name des Softwarepakets einzutragen. Die Beschreibung muß als erstmaliges Anlegen, als Änderung oder als Löschung gekennzeichnet sein. Die datenverarbeitende Stelle hat nach der Verordnung zur Dateibeschreibung (DBeschrV) unverzüglich nach Beginn des Anlegens einer neuen Datei eine Dateibeschreibung zu fertigen. In diesem Fall liegt ein erstmaliges Anlegen vor. Eine Änderung liegt vor, wenn an einer bereits vorhandenen Dateibeschreibung Änderungen vorgenommen wurden, die den Inhalt beeinflussen. Dabei genügt ein Austausch des Deckblatts und ggf. der Blätter, in denen Änderungen auftreten. Werden Freifelder (Leerfelder) belegt, so ist dies ebenfalls zu ändern. Eine Löschung liegt vor, wenn die Datei insgesamt gelöscht wird, weil man die Daten nicht mehr nutzt und ihre Löschungsfrist abgelaufen ist. Sollten Dateien nur vorübergehend gelöscht und später wieder neu angelegt werden (sogenannte saisonale bzw. jährlich wiederkehrende Dateien), so sind diese nicht als gelöscht zu betrachten. Werden nur bestimmte Datenfelder gelöscht, so ist wie bei einer Änderung zu verfahren.

Änderungen und Löschungen sind nach der DBeschrV ebenfalls unverzüglich zu fertigen.

Zu 2. Zweckbestimmung der Datei

In diesem Feld ist der konkrete Zweck der Datei zu beschreiben. Wenn sie Bestandteil eines umfassenden ADV-Verfahrens ist, so sollte dies hier genannt werden. Die Beschreibung muß in allgemeinverständlicher Form den Zweck der Datei erkennen lassen.

Zu 3. Betroffener Personenkreis

Der Personenkreis, über den Daten in der Datei gespeichert sind, ist zu benennen, z. B. Schüler, Patienten, Mitarbeiter oder Empfänger bestimmter Leistungen. Da die Anzahl der betroffenen Personen in der Regel nicht konstant ist, reicht die Angabe eines Wertes, der der durchschnittlichen Größenordnung des Datenbestandes entspricht.

Zu 4. Datenverarbeitung im Auftrag (§ 11 BbgDSG)

Datenverarbeitung im Auftrag liegt vor, wenn die datenverarbeitende Stelle (Auftraggeber) zum Zweck eigener Aufgabenerfüllung einem Auftragnehmer die gesamte Datenverarbeitung oder einzelne Phasen daraus überträgt (siehe auch § 3 Abs. 2 Nr. 1 bis 7 BbgDSG). Der Auftraggeber behält dabei die umfassende Verantwortlichkeit für die Rechtmäßigkeit der Datenverarbeitung (DV), er hat die Ordnungsgemäßheit der DV mit der Auftragserteilung sicherzustellen. Der Auftragnehmer wiederum hat die übertragene Verarbeitung und Nutzung der Daten ausschließlich nach den Weisungen des Auftraggebers durchzuführen.

Liegt keine Auftrags-DV in diesem Sinne vor, ist das Nein-Feld anzukreuzen. Liegt sie vor, ist das Ja-Feld anzukreuzen. Außerdem ist sie als eine von drei Möglichkeiten zu kennzeichnen und mit der Anschrift des Auftragnehmers zu versehen:

- öffentliche Stelle, auf die das BbgDSG Anwendung findet

  Das sind die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes Brandenburg, die Gemeinden und Gemeindeverbände, die der Landesaufsicht unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen.

- öffentliche Stelle, auf die das BbgDSG keine Anwendung findet (Bund, andere Bundesländer)

- nicht-öffentliche Stelle

  Das sind natürliche Personen oder juristische Personen des Privatrechts (Firma, GmbH usw.).

Zu 5. Art der gespeicherten Daten

Die benutzten vorgegebenen Speicherdaten sind zu markieren. Für alle übrigen Felder der Datei sind die Feldbezeichnungen in allgemeinverständlicher Form zu benennen (keine systeminternen Abkürzungen). Dabei können zusammengehörige Datenfelder, die jeweils den gleichen Sachverhalt betreffen, zu Gruppen zusammengefaßt werden, wenn dadurch der Informationsgehalt nicht eingeschränkt wird (z. B. Bankverbindung statt Kontonummer, Bankleitzahl und Kreditinstitut). Reicht der Platz auf dem Formular für die erforderlichen Angaben nicht aus, so sind ein oder mehrere Folgeblätter zu nutzen. Enthält die Datei Freifelder (Leerfelder), so sind diese ebenfalls zu melden. Ferner ist zu vermerken, ob über Schlüsselwörter Verbindungen zu anderen Dateien hergestellt werden können.

Zu 6. bei regelmäßig empfangenen Daten deren Herkunft

Falls Daten regelmäßig empfangen werden (z. B. über Netz, über Datenträgeraustausch oder Formulare), sind deren Art und Herkunft hier einzutragen. Es handelt sich um Datenübermittlungen von Dritten (z. B. durch andere Behörden).

Der Begriff „regelmäßig“ kann sowohl einen sich zeitlich gleichförmig wiederholenden Vorgang als auch einen unkontinuierlichen Vorgang, wenn er nur der „Regel gemäß ist“ (also nach einer vereinbarten Vorschrift abläuft), bedeuten. Eine regelmäßige Übermittlung liegt aber nicht vor, wenn sie nur aufgrund einer konkreten Anfrage im Einzelfall erfolgt.

Zu 7. bei regelmäßig zu übermittelnden Daten deren Empfänger

Falls Daten regelmäßig an Dritte übermittelt werden, sind ihre Art und die (der) Empfänger einzutragen. Zum Begriff der Regelmäßigkeit siehe auch Nummer 6!

Zu 8. Rechtsgrundlage/n der Verarbeitung

Datenverarbeitung ist nach § 3 Abs. 2 BbgDSG das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Die bereichsspezifische Rechtsgrundlage ist zu benennen (z. B. Meldegesetz, Abgabenordnung mit genauer Angabe, z. B.: § 80 Abs. 2 SGB X). Als Rechtsgrundlage gelten Rechtsvorschriften, die in Gesetzen und Rechtsverordnungen enthalten sind. Verwaltungsvorschriften können dagegen nicht als Rechtsgrundlage herangezogen werden.

Zu 9. Fristen für die Sperrung oder Löschung der Daten

Nach § 3 Abs. 2 Nr. 5 BbgDSG ist Sperren (Sperrung) das Verhindern weiterer Verarbeitung gespeicherter Daten; nach Nummer 6 ist Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten. „Sperren" löscht also keine Daten, sondern verbietet ihre weitere Verarbeitung. Dieses Verbot kann später wieder aufgehoben werden. „Löschen" meint dagegen die logische und physikalische Vernichtung der Daten, die nicht mehr rückgängig gemacht werden kann. Falls aus bereichsspezifischen Regelungen Fristen zur Überprüfung der Erforderlichkeiten abzuleiten sind, werden sie hier eingetragen.

Zu 10.1 Kurzbeschreibung der technischen und organisatorischen Maßnahmen gemäß § 10 Abs. 2 BbgDSG

Beispiele für Maßnahmen:

Zugangskontrolle

Festlegung von Sicherungsbereichen, Festlegung von befugten Personen (Mitarbeiter, Fremdbehörden, Fremdfirmen, Wartungsdienste, Anwendungsbetreuung), Besucherregelungen, Sicherung der Räume (Rollos, Schlüssel, Brand- und Bewegungsmelder), Anwesenheitsaufzeichnungen, Außensicherung des Gebäudes durch Schutzzäune, Bewachung, Spezialverglasung der Fenster, elektrische Türöffner, Fernsehmonitor

Datenträgerkontrolle

Datenträgerverwaltung einschließlich Protokollierung der Befugten, Periodizität der Bestandskontrollen, Datenträgervernichtungsprotokollierung, Einschränkung von Softwaremöglichkeiten zum Kopieren von Dateien und Datenträgern, Festlegungen zum Kopieren von Dateien und zu Datensicherungsmaßnahmen, vielleicht Datenverschlüsselung, Festlegungen zur Aufbewahrung von Datenträgern

Speicherkontrolle

Festlegungen der Befugnisse für die Eingabe, Kenntnisnahme, Veränderung und Löschung der Daten, Zuordnung der Arbeitsplätze (z. B. Systemverwalter, Arbeitsstationen), Festlegungen zur Programmfreigabe, Protokollierung der Dateienbenutzung, Richtlinien zur Dateiverwaltung, Wartung und Fernwartung, zur Arbeit des Systemverwalters

Benutzerkontrolle

Abschließbarkeit oder Verplomben der Datenstationen, Vergabe von Benutzerpaßwörtern und Festlegung zu deren Wechsel, evtl. Verschlüsselung der Paßwörter, Festlegungen zu Datenübertragungen bei Netzarbeit (Abschottung von anderen Netzen, Begrenzung der Netzverwaltung auf 1 oder 2 Nutzer, Festlegung, welche Daten sollen wie übertragen werden)

Zugriffskontrolle

Fixierung der benutzerspezifischen, abgestuften Rechteverwaltung auf Unterverzeichnis- und Dateiebene, wodurch die Einschränkung der Zugriffsmöglichkeiten auf die Aufgabenerfüllung erreicht wird (Benutzerkennzeichen und Paßwort, interne/externe Dateizugriffe, Festlegung zum Lesen, Schreiben, Löschen, ferner zum Satz- und Feldschutz), Systemverwaltung u. U. nach dem 4-Augen-Prinzip, Bildschirmverdunkelung bei Arbeitsunterbrechung (Weiterarbeit u. U. erst nach Wiedereingabe des Paßworts), regelmäßige Überprüfung der festgelegten Befugnisse bezüglich Zugriffsrechten, Wartung nur in Anwesenheit des Systemverwalters, eindeutige Identifizierung der Ein- und Ausgabegeräte im Netzverband

Übermittlungskontrolle

Festlegung der zugelassenen Übermittlungsberechtigten (Sender), Übermittlungsempfänger und Übermittlungswege, Kontrolle der Empfangsberechtigung, Festlegung einer ausreichenden Benutzeridentifizierung (Zeiten, Personen, Verfahren, Geräte, Programme, welche Daten), Vorgangsprotokollierung aller Datenübertragungen und Festlegungen zur Auswertung der Protokolle (Periodizität, Umfang); falls überhaupt Fernwartung, dann Sicherstellung, daß personenbezogene Daten nicht eingesehen werden können, Protokollierung und Anzeige der Aktivitäten auf dem Bildschirm in Anwesenheit des Systemverwalters; Festlegung, ob die zu übertragenden Daten zu verschlüsseln sind (Verfahren); Festlegung über Freigabe von Programmen zur Datenübermittlung

Eingabekontrolle

Festlegung, wer Daten eingeben darf; Kennzeichnung von Erfassungsunterlagen mit Namen und Datum nach Vollzug der Eingabe; Protokollierung der Netzverwaltung, der Lese- und Schreibzugriffe auf Dateien und der gescheiterten Zugriffsversuche, der Programmaufrufe; Auswertung der Protokolle und Festlegung, zu welchen Zwecken sie verwendet werden dürfen; Festlegung zu Veränderungen von Zugriffsrechten und zur Dateiverantwortlichkeit

Auftragskontrolle

Diese Angaben sind nur erforderlich, wenn tatsächlich Datenverarbeitung im Auftrag durchgeführt wird (siehe auch Nummer 4). Ist dies der Fall, dann gilt das Prinzip, daß beim Auftragnehmer dieselben Sicherheitsmaßnahmen angewandt werden müssen wie bei eigener Datenverarbeitung.

Nach § 11 BbgDSG ist diese Beauftragung in Schriftform abzuschließen (Vertrag) und zustimmungsabhängig. Im Vertrag sollten geregelt sein: die Festlegung der Kompetenzen und Pflichten von Auftragnehmer und Auftraggeber, Vereinbarungen über Kündigungsmöglichkeiten, Vertragsstrafen und Kontrollrechte für den Auftraggeber, ferner bei Programmieraufträgen das Pflichtenheft, Testvorführungen und Programmfreigabe u. a.

Transportkontrolle

Übertragung von personenbezogenen Daten (über Netze): Festlegungen zum Abschirmen von Kabeln zwecks höherer Abhörsicherheit, zur Verschlüsselung von Daten (Verfahren), Art der Übertragungswege und der festgelegten Verfahren

Übertragung beim Transport von Datenträgern: Festlegungen zu der zum Transport berechtigten Personen, zu Begleitpapieren, zu Verpackungs- und Versandvorschriften. Bei Rückgabe von magnetischen Datenträgern vorher Löschen der nicht mehr benötigten personenbezogenen Daten durch physikalisches Überschreiben (evtl. mehrmaliges Formatieren). Gleiches gilt für die zur Vernichtung vorgesehenen Datenträger; auch Entmagnetisieren ist sinnvoll. Für die Vernichtung von Akten und Mikrofilmen gilt DIN 32757.

Organisationskontrolle

Stellenbeschreibungen, Erstellung der Dienstanweisung bezüglich Datenschutz, Festlegung der Personen, die deren Einhaltung überprüfen, schriftliche Verpflichtung auf das Datengeheimnis, Regelungen zu Auskunftsmitteilungen aus personenbezogenen Datenbeständen, Beschreibung der Aufgaben des Systemverwalters, Festlegungen zu Datensicherungsmaßnahmen, Regelungen für: Festlegung des Aktenplanes, der Ordnung der Ablage, der Aufbewahrung von Unterlagen und Protokollen, Arbeitsordnung für die kontrollierte Datenträgervernichtung (Unterlagen, Akten, Listen, Fehldrucke, Testdrucke, Magnetbänder und -platten, Disketten, Mikrofilme, CD-ROM, Videofilme usw.), Regelung der Meldung automatisierter Abrufverfahren an den Landesbeauftragten für Datenschutz, Beachtung der Mitbestimmungsrechte des Personalrats bei der automatisierten Verarbeitung von Personaldaten gemäß Landespersonalvertretungsgesetz, Beschreibung der Aufgaben und Kompetenzen des behördlichen Datenschutzbeauftragten, Regelungen für Havariefälle bei der ADV (Notvarianten u. a.), Anwendung eines Schutzstufenkonzepts zur Festlegung der Sensibilität von personenbezogenen Daten

Zu 10.2 Ist einer Organisationseinheit die Überprüfung von Art und Umfang der getroffenen Datensicherungsmaßnahmen übertragen?

Es ist zu vermerken, ob die unter Nummer 10.1 festgelegten Maßnahmen von einer Organisationseinheit und von welcher auf ihren Inhalt überprüft werden.

Zu 10.3 Ist einer Organisationseinheit die Kontrolle der Einhaltung der zur Datensicherung bestehenden Vorschriften und Anweisungen übertragen?

Es ist zu vermerken, ob einer und welcher Organisationseinheit die laufende Kontrolle der getroffenen Sicherungsmaßnahmen übertragen wurde.

Zu 10.4 Gibt es eine Dienstanweisung für die Datensicherung?

Es ist anzugeben, ob eine und welche Dienstanweisung existiert.

Zu 10.5 Existiert zu der Datei eine Paralleldatei mit fiktiven Daten zu Schulungs-, Test- und Servicezwecken?

Falls Paralleldateien existieren, ist dies einzutragen und der Dateiname anzugeben.

Zu 11. Beschreibung des automatisierten Verfahrens (Kurzbeschreibung)

Kurze inhaltliche Darstellung des Verfahrens, auch Angabe der Programmsprache oder Name des Softwareprodukts.

Zu 11 a Betriebsart des Verfahrens

Vermerken, ob Stapel- oder Dialog-Betrieb oder eine andere Betriebsart angewandt wird.

Zu 11 b Art der Geräte

Vermerken, ob es sich um Großrechner, Arbeitsplatzrechner oder Mehrplatzsystem, Arbeitsplatzrechner oder Einplatzsystem oder um andere Geräte handelt.

Zu 11 c Stellen, bei denen die Geräte aufgestellt sind

Angaben mit Anschrift, falls der Aufstellungsort von der speichernden Stelle abweicht, sonst Angaben zu Abteilungen und Räumen.

Zu 11 d Verfahren (auch bei auftragsweiser Datenverarbeitung) zur

- Übermittlung

  Falls eine Übermittlung von Daten erfolgt, ist zu vermerken, ob diese durch Datenträgeraustausch (z. B. Magnet-

bänder, Disketten, Eingabebelege, Ausdrucke) erfolgt oder durch Leitungsübertragung (Netze). Diese ist nach Art (z. B. File-Transfer, Stapelverarbeitung, Dialog-Datenverarbeitung), Typ (z. B. Wählleitung über Steuereinheit, Knotenrechner, Modem; Standleitung; Datenfunk), Prozedur (z. B. Transdata/Siemens, SNA/IBM, TCP/IP, X.25, ISDN o. a.) und priv./öffentliches Netz (z. B. Postdienst: Fernsprechdienst, DATEX-L, DATEX-P, Direktrufnetz oder privater Anbieter) kurz zu beschreiben.

- Sperrung

  Nur notwendig, falls besondere Festlegungen getroffen wurden.

- Löschung

  Nur notwendig, falls besondere Festlegungen getroffen oder rechtlich vorgegeben sind.

- Auskunftserteilung

  Hier ist ein möglicherweise vorgesehenes Verfahren zur Auskunftserteilung an den Betroffenen zu erläutern.

Anlage 3

Hinweise zum Ausfüllen der Formulare zum Geräteverzeichnis

Für jede Rechner-Zentraleinheit ist ein getrenntes Formular zu verwenden.

Zu 1. Rechner-Zentraleinheit

Typ des Rechners: Es wird angekreuzt, ob es sich um einen Arbeitsplatzcomputer, ein Mehrplatzsystem (auch Netzserver) oder einen Großrechner handelt

Hersteller: Eintrag des Firmennamens

Betriebssystem: Name des Systems (z. B. MS-DOS, UNIX, Windows NT, MVS, BS2000)

Kapazität des Arbeitsspeichers:
Angabe des Rechner-Hauptspeichers in Kilo- oder Megabyte

Zu 2. Peripherie des Rechners

Es ist die Anzahl der angeschlossenen Terminals, der Drucker und sonstiger Ein- oder Ausgabegeräte anzugeben.

Zu 3. Vernetzung des Rechners

Die Angaben unter Nummer 3 sind nur zu machen, wenn tatsächlich eine Vernetzung (lokal oder weitläufig) vorliegt.

Zu 3.1 Angaben nur für lokales Netz

Hier sind der Typ (z. B. Ethernet-Bus) und das Netz-Betriebssystem (z. B. Novell NetWare) anzugeben.

Zu 3.2 Einrichtungen zur Datenfernverarbeitung und -übertragung

Diese sind für jede Einrichtung anzugeben, die einer Fernverarbeitung dienen, und zwar nach Art (z. B. File-Transfer, Stapelverarbeitung, Dialogverarbeitung), nach Typ (z. B. Wählleitung über Steuerrechner, Knotenrechner, Modem; Standleitung; Datenfunk), nach Prozedur (z. B. Transdata/Siemens, SNA/IBM, TCP/IP, X.25, ISDN o. a.), nach Postdienst (falls dieser genutzt wird: z. B. Fernsprechnetz, DATEX-L, DATEX-P, Direktrufnetz) und nach Empfänger (Name, Anschrift).

Zu 4. Programm zur Verarbeitung personenbezogener Daten

Es sind alle Programme zu notieren, mit denen auf diesem Rechner personenbezogene Daten verarbeitet werden, und zwar mit Programm-Name, Hersteller (Eigen- oder Fremdprogrammierung) und der benutzten Standardsoftware (Name).

Anlage 4

Regeln zum sicheren Umgang mit dem Arbeitsplatzcomputer (APC)

1. **Schützen Sie den APC vor der Benutzung durch Unbefugte und verhindern Sie beim Verlassen des Arbeitsplatzes die unberechtigte Benutzung von Programmen und Daten**

   Maßnahmen:
   - Machen Sie Gebrauch vom Tastaturschloß.
   - Schließen Sie Ihr Dienstzimmer beim Verlassen ab.
   - Schalten und schließen Sie den APC ab oder schließen Sie ihn ein.

2. **Gehen Sie verantwortungsvoll mit den vorgesehenen Schutzmöglichkeiten des APC um und verhindern Sie die Kenntnisnahme von Daten bei der Eingabe oder Ausgabe**

   Maßnahmen:
   - Halten Sie das Paßwort geheim.
   - Benutzen Sie „gute“ Paßwörter und wechseln Sie diese öfter.

- Lassen Sie sich bei der Arbeit an der Tastatur und Bildschirm (vor allem bei der Eingabe des Paßwortes) nicht von Unbefugten beobachten.
- Schließen Sie nicht verwendete Ausdrucke ein oder vernichten Sie diese.

3. Verhindern Sie die Beschädigung und den Diebstahl von beweglichen Datenträgern (Disketten, Wechselplatten)

Maßnahmen:
- Bewahren Sie Disketten in ihren Hüllen und möglichst senkrecht stehend auf.
- Knicken und drücken Sie Disketten nicht.
- Halten Sie die Datenträger von magnetischen Feldern (Bildschirm, elektrische Geräte) fern.
- Schließen Sie die Datenträger bei Nichtbenutzung ein oder geben Sie diese an das Archiv zurück.
- Beschriften Sie die Etiketten der Datenträger eindeutig und aussagekräftig.

4. Schützen Sie Programme und Daten vor einer unbeabsichtigten Zerstörung

Maßnahmen:
- Lassen Sie Datenträger nur solange im Laufwerk wie nötig.
- Nutzen Sie den mechanischen Schreibschutz auf Datenträgern (z. B. Kippschalter auf der Rückseite einer Diskette).

5. Benutzen Sie im Dienst keine private Hard- und Software und die dienstliche Hard- und Software nur am Arbeitsplatz

Maßnahmen:
- Benutzen Sie nur freigegebene Rechner, Datenträger und Programme.
- Machen Sie keine unerlaubten Kopien von Daten und Programmen.
- Spielen Sie keine fremden oder privaten Programme von Datenträgern ein.

6. Schützen Sie Programme und Daten vor dem mißbräuchlichen Lese- und Schreibzugriff durch andere APC-Benutzer

Maßnahmen:
- Gestatten Sie den Zugriff auf Dateien nur den Personen, für die er notwendig ist.
- Gestatten Sie nur die Art des Zugriffs, die unbedingt nötig ist und nur für einen bestimmten Zeitraum.

7. Löschen Sie Daten auf beweglichen Datenträgern, die nicht mehr benötigt werden, immer durch vollständiges Überschreiben der alten Daten

Maßnahmen:
- Löschen Sie Dateien immer durch vollständiges Überschreiben der zu löschenden Datei.
- Lassen Sie unbrauchbare oder auszusondernde Datenträger durch mechanische oder andere physikalische Zerstörung vernichten.

8. Schützen Sie sich durch ordnungsgemäße Datensicherung gegen Auswirkungen von Programm- und Datenverlust

Maßnahmen:
- Sichern Sie alle Verarbeitungsdaten regelmäßig auf Sicherungskopien (z. B. nach dem 3-Generationen-Prinzip).
- Machen Sie von Programmen eine Sicherungskopie der Originalversion.
- Bewahren Sie die Sicherungsdatenträger getrennt von den Arbeitskopien auf.

9. Überprüfen Sie regelmäßig Geräte, Verbindungen und Datenbestände auf nicht beabsichtigte oder unverständliche Änderungen

Maßnahmen:
- Achten Sie auf verändertes Programm- und Systemverhalten beim Beginn und während der Arbeit.
- Überprüfen Sie regelmäßig die Datenbestände auf Unversehrtheit.

10. Informieren Sie die systembetreuende Stelle oder den Sicherheitsbeauftragten entsprechend der Hausanordnung über ungewöhnliche Ereignisse

Maßnahmen:
- Melden Sie unerwartetes Verhalten der Systembetreuung in Ihrer Behörde.
- Melden Sie ungewöhnliche Ereignisse dem Sicherheitsbeauftragten.

Zusammenschluß der Gemeinden Schönborn, Lindena, Gruhno und Schadewitz zu einer neuen Gemeinde Schönborn

Bekanntmachung des Ministeriums des Innern
Vom 23. Dezember 1997

Das Ministerium des Innern hat in Anwendung von § 9 Abs. 3 Satz 3 der Gemeindeordnung für das Land Brandenburg vom 15. Oktober 1993 (GVBl. I S. 398) den Zusammenschluß der Gemeinden

Schönborn, Lindena, Gruhno und Schadewitz
(Landkreis Elbe-Elster/Amt Elsterland)
zu einer neuen Gemeinde Schönborn

genehmigt.

Die Bildung der neuen Gemeinde wird am Tag der landesweiten Kommunalwahl im Jahr 1998 wirksam.

Die Schlüsselnummer der neuen Gemeinde lautet:

12 0 62 453

Auslandsumzugskostenverordnung - AUV - - Durchführungsvorschriften des Auswärtigen Amts und des Bundesministeriums des Innern zur AUV -

Rundschreiben des Ministeriums der Finanzen
15.3 - 2723 - 2
Vom 22. Dezember 1997

Dem Ministerium der Finanzen - Referat 15 - werden Rundschreiben des Auswärtigen Amts (AA) zur Durchführung einzelner oder mehrerer Vorschriften der AUV übersandt.

Aufgrund der geringen Zahl von Anwendungsfällen der AUV im Land Brandenburg werde ich wie bisher auch zukünftig grundsätzlich von der Bekanntgabe und Übersendung eines Abdrucks dieser Rundschreiben für den Landesbereich Abstand nehmen, sondern nur einen Hinweis auf deren Bekanntmachung im Gemeinsamen Ministerialblatt der Bundesministerien (GMBl) im Amtsblatt für Brandenburg veröffentlichen.

Sollte allerdings ein dringender Anwendungsbedarf bestehen, werde ich benötigte Durchführungsvorschriften auf Anforderung übersenden.

Nachstehende Durchführungsvorschriften des Auswärtigen Amts bzw. des Bundesministeriums des Innern liegen mir bereits vor:

1. Richtlinien des Auswärtigen Amts für die Erstattung der Transportversicherungskosten bei Auslandsumzügen (RLTV) vom 1. Oktober 1997 (GMBl S. 730) einschließlich der im GMBl nicht abgedruckten Anlagen A sowie C 1 bis C 5

2. Erläuterungen und Hinweise des Auswärtigen Amts zur Durchführung der Auslandsumzugskostenverordnung nach dem Stand der AUV vom 1. September 1997 (RdSchr. des AA vom 12. November 1997 - 113 - 9 - 4 - 134.00)

3. Wohnungsbesichtigungs- und Umzugsabwicklungsreisen nach § 4 Abs. 4 AUV (RdSchr. des AA vom 1. Dezember 1997 - 113 - RL (9 - 50) - 134.30/1)

4. Unverzinslicher Gehaltsvorschuß bei Verwendung im Ausland (RdSchr. des BMI vom 24. September 1997 - GMBl S. 566).

Richtlinie des Ministeriums für Ernährung, Landwirtschaft und Forsten über die Gewährung von Zuwendungen aus den Mitteln der Walderhaltungsabgabe und ihre Verwendung zum Zwecke der Erhaltung des Waldes

Vom 23. Dezember 1997

1. Zuwendungszweck, Rechtsgrundlage

Das Land gewährt Zuwendungen zum Zwecke der Walderhaltung nach Maßgabe dieser Richtlinie und der Verwaltungsvorschriften zu § 44 der Landeshaushaltsordnung (VV zu § 44 LHO).

Ein Anspruch des Antragstellers auf Gewährung der Zuwendung besteht nicht, vielmehr entscheidet die Bewilligungsbehörde aufgrund ihres pflichtgemäßen Ermessens im Rahmen der verfügbaren Haushaltsmittel aus der Walderhaltungsabgabe.

2. Gegenstand der Förderung

Soweit nicht andere Förderrichtlinien anwendbar sind, können insbesondere nachfolgende Maßnahmen gefördert werden.

2.1 Freiwilliger Tausch von Grundstücken mit dem Ziel der Erstaufforstung in den Gebieten, in denen aus landespflegerischen Gründen ein höherer Waldanteil anzustreben ist

2.2 Erstaufforstung von Grundstücken in Gebieten, in denen aus landespflegerischen Gründen ein höherer Waldanteil anzustreben ist

2.3 Aufforstung und Erstaufforstung von Grundstücken in Gebieten, wo eine Erhöhung des Laubholzanteiles dringend notwendig ist

2.4 Maßnahmen zur Verbesserung und Stabilisierung des Waldes

2.5 Maßnahmen zur Waldbrandvorbeugung und Beseitigung von Waldbrandfolgen

2.6 Waldschutzmaßnahmen gegen tierische, pflanzliche und andere Schädlinge sowie gegen schädigende Naturereignisse

2.7 Rekultivierung von Flächen mit Landschaftsschäden zum Zwecke der Aufforstung, soweit eine rechtliche Verpflichtung Dritter zur Rekultivierung nicht besteht oder nicht durchsetzbar ist

3. Zuwendungsempfänger

3.1 Land- und forstwirtschaftliche Unternehmen, sofern die Kapitalbeteiligung der öffentlichen Hand nicht mehr als ein Viertel beträgt

3.2 Juristische Personen des öffentlichen und privaten Rechts mit Ausnahme des Bundes und der Länder

3.3 Anerkannte forstwirtschaftliche Zusammenschlüsse

4. Zuwendungsvoraussetzungen

Die Maßnahme darf nicht durch andere Förderrichtlinien förderbar sein oder bereits gefördert werden.

Die zu fördernde Maßnahme muß dem Zweck der Erhaltung des Waldes im Land Brandenburg im weitesten Sinne dienen. Sofern dies nicht deutlich aus der Bezeichnung der Maßnahme hervorgeht, ist eine Erläuterung beizufügen (vgl. Nummer 7.1).

5. Art und Umfang, Höhe der Zuwendung

5.1 Zuwendungsart: Projektförderung

5.2 Finanzierungsart: Anteilfinanzierung

Bagatellgrenze: 5000 DM

5.3 Form der Zuwendung

Die Zuwendung wird in Form eines einmaligen Zuschusses gewährt.

5.4 Bemessungsgrundlage

5.4.1 Maßnahmen zur Bekämpfung von nadel- und blattfressenden Insekten

Die Maßnahmen müssen von der Landesforstverwaltung bestätigt sein oder durch diese selbst durchgeführt werden. Sie müssen fachlich richtig sein und rechtzeitig eingeleitet werden.

Grundlage für die Bemessung sind die Größe der Waldfläche des Waldbesitzers (Antragsteller) sowie die Bekämpfungskosten.

Der Zuschuß kann betragen:

bis 200 ha Waldfläche bis zu 70 v. H. der Bekämpfungskosten

über 200 ha bis 800 ha Waldfläche bis zu 50 v. H. der Bekämpfungskosten

In Abstimmung mit der obersten Forstbehörde kann die Bewilligungsbehörde bei ungünstigen Standorten, bei Flächen mit neuartigen Waldschäden oder bei Betrieben mit überdurchschnittlicher Ausstattung mit Jungbeständen in begründeten Einzelfällen Ausnahmen zulassen.

Für Fälle der akuten Gefahrenabwehr können die Maßnahmen begonnen oder abgeschlossen sein.

5.4.2 Übrige Maßnahmen

Grundlage für die Bemessung der Zuwendung bildet der im Antrag kalkulierte Kostenvoranschlag für die Maßnahme. Die Kostenkalkulation ist Bestandteil des Antrages. Der Zuschuß kann bis zu 70 v. H. betragen.

In Abstimmung mit der obersten Forstbehörde kann die Bewilligungsbehörde bei ungünstigen Standorten, bei Flächen mit neuartigen Waldschäden oder bei Betrieben mit überdurchschnittlicher Ausstattung mit Jungbeständen in begründeten Einzelfällen Ausnahmen zulassen.

6. Sonstige Zuwendungsbestimmungen

keine

7. Verfahren

7.1 Antragsverfahren

Der Antrag an die Bewilligungsbehörde ist nach dem Grundmuster der VV zu § 44 LHO zu stellen. Zur vorgesehenen Maßnahme ist eine Erläuterung zu geben, sofern die Bezeichnung der Maßnahme sowie die Begründung zur Notwendigkeit der Maßnahme nicht den Zweck der Walderhaltung ausreichend deutlich werden lassen.

7.2 Bewilligungsverfahren

Der Antrag ist an das örtlich zuständige Amt für Forstwirtschaft einzureichen. Die Ämter für Forstwirtschaft sind Bewilligungsbehörde.

Die Bewilligungsbehörde prüft den Antrag und gibt dem Antragsteller einen Zuwendungsbescheid. Der Verwendungsnachweis ist gegenüber der Bewilligungsbehörde zu führen.

Für die Bewilligung, Auszahlung und Abrechnung der Zuwendung sowie für den Nachweis und die Prüfung der Verwendung und die ggf. erforderliche Aufhebung des Zuwendungsbescheides und die Rückforderung der gewährten Zuwendung gelten die VV/VVG zu § 44 LHO, soweit nicht in dieser Förderrichtlinie Abweichungen zugelassen worden sind.

8. Inkrafttreten, Geltungsdauer

Diese Richtlinie tritt mit Wirkung vom 1. Januar 1998 in Kraft und ist bis zum 31. Dezember 1999 befristet.

Die Richtlinie über die Gewährung von Zuwendungen aus den Mitteln der Walderhaltungsabgabe und ihre Verwendung zum Zwecke der Erhaltung des Waldes vom 17. Februar 1995 (ABl. S. 286) tritt am 1. Januar 1998 außer Kraft.

Erlaß des Ministeriums für Stadtentwicklung, Wohnen und Verkehr zur Förderung der behindertengerechten Anpassung von Mietwohnungen (Wohnraumanpassungserlaß)

Änderungserlaß des Ministeriums für Stadtentwicklung, Wohnen und Verkehr
Vom 8. Januar 1998

1. Der Erlaß zur Förderung der behindertengerechten Anpassung von Mietwohnungen, Runderlaß des Ministers für Stadtentwicklung, Wohnen und Verkehr vom 18. April 1996 (ABl. S. 520), wird wie folgt geändert:

   Nummer 10 Satz 1 lautet: „Die Geltungsdauer dieses Erlasses ist bis zum 31. Dezember 1999 befristet.“ Satz 2 entfällt.

2. Dieser Änderungserlaß tritt mit Wirkung vom 31. Dezember 1997 in Kraft.

A 11271 Postvertriebsstück – Entgelt bezahlt

Amtsblatt für Brandenburg
Gemeinsames Ministerialblatt für das Land Brandenburg

Herausgeber: Minister des Innern des Landes Brandenburg.
Der Bezugspreis beträgt jährlich 110,– DM (zzgl. Versandkosten + Portokosten). Die Preise enthalten keine Mehrwertsteuer, da die Herausgabe Amtsblattes hoheitliche Tätigkeit ist. Die Einweisung kann jederzeit erfolgen.
Die Berechnung erfolgt im Namen und für Rechnung des Ministeriums des Innern des Landes Brandenburg.
Die Kündigung ist nur zum Ende eines Bezugsjahres zulässig; sie muß bis spätestens 3 Monate vor Ablauf des Bezugsjahres dem Verlag zugegangen sein.
Die Lieferung dieses Blattes erfolgt durch die Post. Reklamationen bei Nichtzustellung, Neu- bzw. Abbestellungen, Änderungswünsche und sonstige Anforderungen sind an die Brandenburgische Universitätsdruckerei und Verlagsgesellschaft Potsdam mbH zu richten.
Herstellung, Verlag und Vertrieb: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft Potsdam mbH, Karl-Liebknecht-Straße 24–25, Haus 2, 14476 Golm (bei Potsdam), Telefon Potsdam 56 89 - 0