BEKANNTMACHUNGEN DER LANDESBEHÖRDEN

Verwaltungsvorschrift des Ministeriums des Innern zur Durchführung des Brandenburgischen Datenschutzgesetzes (VV-BbgDSG)

Vom 14. Dezember 2010

1 Inhaltsverzeichnis

2 Zu § 2 Anwendungsbereich

2.1 In § 2 BbgDSG wird der von der Aufgabenwahrnehmung beziehungsweise Organisationsform von Stellen der öffentlichen Verwaltung abhängige Anwendungsbereich des Brandenburgischen Datenschutzgesetzes (BbgDSG) geregelt. Je nach Organisationsform beziehungsweise konkreter Aufgabenwahrnehmung haben öffentliche Stellen nach Absatz 1 das Brandenburgische Datenschutzgesetz uneingeschränkt anzuwenden. Stellen nach Absatz 2 haben das Brandenburgische Datenschutzgesetz nur bezüglich der Aufgabenwahrnehmungen anzuwenden, die nicht den wirtschaftlichen Zwecken oder Zielen dienen. Hinsichtlich der Aufgabenwahrnehmung im Bereich der wirtschaftlichen Betätigung haben diese Stellen die Vorschriften des Bundesdatenschutzgesetzes (BDSG) für nicht-öffentliche Stellen anzuwenden. Privatrechtlich organisierte Stellen haben immer das Bundesdatenschutzgesetz anzuwenden, soweit sie nicht als Beliehene hoheitliche Aufgaben wahrnehmen.

2.2 Absatz 1 legt den Anwendungsbereich des Gesetzes und die Ausnahmen hiervon fest. Dabei kommt es grundsätzlich nur auf die Eigenschaft des Adressaten als einer öffentlichen Stelle an. Diese Eigenschaft hängt von der gewählten Organisationsform ab. Mit der Regelung wird der gesamte öffentlich-rechtliche Organisationsbereich des Landes in den Anwendungsbereich des Gesetzes einbezogen. Unerheblich ist, ob die öffentliche Stelle hoheitlich oder fiskalisch handelt. Privatrechtlich organisierte Stellen sind immer nicht-öffentliche Stellen.

2.3 Behörde ist jede organisatorisch selbstständige Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt (vergleiche § 1 Absatz 2 des Verwaltungsverfahrensgesetzes für das Land Brandenburg [VwVfGBbg]), wobei die organisatorische Selbstständigkeit der Behörde am eigenverantwortlichen Auftreten nach außen zu erkennen ist. Sonstige öffentliche Stellen sind nach außen eigenverantwortlich handelnde Stellen, die keine Behördeneigenschaft besitzen, zum Beispiel öffentlich-rechtliche Wettbewerbsunternehmen. Vereinigungen juristischer Personen des öffentlichen Rechts sind nur dann öffentliche Stellen, wenn sie öffentlich-rechtlich organisiert sind. Amtsträger oder Dienststellen, die nach den maßgeblichen organisatorischen Bestimmungen nur im Namen und mit Wirkung für und gegen andere Stellen handeln können, insbesondere Ämter, Sachgebiete, Dezernate, Referate und Abteilungen einer Behörde, sind nicht selbst Behörde oder öffentliche Stelle im Sinne dieses Gesetzes.

2.4 Gerichte und Staatsanwaltschaften unterliegen dem Brandenburgischen Datenschutzgesetz nur, soweit sie Verwaltungsaufgaben wahrnehmen. Im Bereich der Rechtsprechung gelten die Bestimmungen der einschlägigen Prozessordnungen. Soweit die Staatsanwaltschaften Aufgaben der Strafverfolgung wahrnehmen, finden nur die Bestimmungen nach Abschnitt 2 des Gesetzes Anwendung.

2.5 Nehmen nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr (sogenannte beliehene Unternehmen), gelten sie insoweit als öffentliche Stel-

len, vergleiche § 1 Absatz 2 VwVfGBbg. Im Rahmen dieser Tätigkeit gilt das Brandenburgische Datenschutzgesetz (§ 2 Absatz 1 Satz 3 BbgDSG). Der den Regelungen des Brandenburgischen Datenschutzgesetzes unterliegende Tätigkeitsbereich ergibt sich aus dem Beleihungsakt.

2.6 Soweit kommunale Gebietskörperschaften Eigengesellschaften (rechtlich selbstständige Unternehmen in zivilrechtlichen Formen wie Aktiengesellschaften oder Gesellschaften mit beschränkter Haftung) errichten oder an privatrechtlich organisierten wirtschaftlichen Unternehmen beteiligt sind, sind für solche Unternehmen - sofern sie nicht als Beliehene tätig werden - die Vorschriften bezüglich der Datenverarbeitung durch nicht-öffentliche Stellen uneingeschränkt anzuwenden.

2.7 Die in § 2 Absatz 2 BbgDSG genannten wirtschaftlichen Unternehmen und sonstigen Einrichtungen, die überwiegend wirtschaftliche Aufgaben wahrnehmen beziehungsweise am Wettbewerb teilnehmen, werden hinsichtlich der materiellen Datenschutzregelungen weitgehend wie private Stellen behandelt. Als wirtschaftliche Betätigung im Sinne des Brandenburgischen Datenschutzgesetzes ist das Herstellen, Anbieten oder Verteilen von Gütern, Dienstleistungen oder vergleichbaren Leistungen, die ihrer Art nach auch mit der Absicht der Gewinnerzielung erbracht werden könnten, anzusehen. Soweit die in § 2 Absatz 2 BbgDSG genannten Stellen personenbezogene Daten in Ausübung ihrer wirtschaftlichen Tätigkeit verarbeiten, kommen nur die in Absatz 2 Satz 1 genannten Vorschriften des Brandenburgischen Datenschutzgesetzes zur Anwendung. Im Übrigen unterliegen diese Stellen den Vorschriften des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen. Stellen nach Absatz 2 Satz 2 sind unter anderem die Eigenbetriebe nach § 93 der Kommunalverfassung und die öffentlichen Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden. Für Landesbetriebe nach § 26 der Landeshaushaltsordnung (zum Beispiel der Brandenburgische IT-Dienstleister [ZIT-BB] oder der Landesbetrieb „Landesvermessung und Geobasisinformation Brandenburg“ [LGB]) finden die Vorschriften des Brandenburgischen Datenschutzgesetzes ebenfalls nur eingeschränkt Anwendung.

2.8 Zu den juristischen Personen des öffentlichen Rechts, die der Aufsicht des Landes unterliegen und am Wettbewerb teilnehmen, zählen unter anderem Sparkassen und die Ortskrankenkasse (AOK).

2.9 Öffentlich-rechtlich organisierte Krankenhäuser gehören zu den Einrichtungen im Sinne des § 2 Absatz 2 Satz 1 Nummer 1 BbgDSG, die am Wettbewerb teilnehmen und für die die Vorschriften des Brandenburgischen Datenschutzgesetzes nur eingeschränkt gelten. Dies gilt jedoch nicht, soweit Krankenhäuser hoheitliche Aufgaben (zum Beispiel im Rahmen von Zwangseinweisungen) wahrnehmen. Für privatrechtlich organisierte Krankenhäuser gelten neben den vorrangig zu beachtenden krankenhausrechtlichen Vorschriften (zum Beispiel des Brandenburgischen Krankenhausentwicklungsgesetzes) ausschließlich die Vorschriften des Bundesdatenschutzgesetzes.

2.10 Für die Verarbeitung personenbezogener Daten der Beschäftigten der in Absatz 2 genannten Stellen ist das Brandenburgische Datenschutzgesetz anwendbar, da diese nicht unmittelbar wirtschaftlichen Zwecken dient und die Daten damit nicht in Ausübung wirtschaftlicher Tätigkeit verarbeitet werden.

2.11 In Absatz 4 ist das Verhältnis zwischen dem Verwaltungsverfahrensgesetz für das Land Brandenburg und dem Brandenburgischen Datenschutzgesetz geregelt. Das Datenschutzgesetz hat Vorrang, wenn es in einem Verwaltungsverfahren um die Ermittlung des Sachverhalts geht. Soweit die Verwaltungstätigkeit nicht in der Ermittlung des Sachverhalts besteht, gelten die Vorschriften des Verwaltungsverfahrensgesetzes uneingeschränkt. Dies kann sowohl bedeuten, dass abweichende Vorschriften Vorrang haben als auch, dass andere Vorschriften nebeneinander gelten. Zu den Vorschriften die Vorrang haben, gehört § 29 VwVfG in Verbindung mit § 1 Absatz 1 VwVfGBbg, der bestimmt, unter welchen Voraussetzungen den Beteiligten Akteneinsicht in laufenden Verwaltungsverfahren gewährt wird. In Fällen der Amtshilfe gelten die Vorschriften des Brandenburgischen Datenschutzgesetzes und des Verwaltungsverfahrensgesetzes für das Land Brandenburg nebeneinander beziehungsweise ergänzen sich.

3 Zu § 3 Begriffsbestimmungen

3.1 Personenbezogene Daten im Sinne von Absatz 1 sind Einzelangaben, die eine natürliche lebende Person (Betroffener) bestimmen oder bestimmbar machen (zum Beispiel Name, Personalnummer, Kfz-Kennzeichen). Als Einzelangaben gelten weiterhin Daten, die einen in der Person des Betroffenen liegenden oder auf den Betroffenen bezogenen Sachverhalt beschreiben (zum Beispiel Adresse, Einkommen, Familienstand, Geburtsdatum, Staatsangehörigkeit, Krankheit, Zeugnisnoten, Berufsbezeichnung, Eigentum); auch Werturteile und Bildnisse gehören dazu. Einzelangaben in diesem Sinne sind nicht nur Daten, an deren Geheimhaltung die Betroffenen ein Interesse haben (Geheimnisse), sondern jedwede Angaben zur Person.

3.2 Nicht personenbezogen und damit vom Schutzbereich des Gesetzes nicht erfasst sind Daten über juristische Personen (AG, KG auf Aktien, GmbH) oder über Personenvereinigungen (zum Beispiel offene Handelsgesellschaften, nicht rechtsfähige Vereine), soweit kein Rückschluss auf eine natürliche Person möglich ist. Dieser Rückschluss ist nicht gegeben, soweit eine natürliche Person nur in ihrer Eigenschaft als Organ oder zum Beispiel als Geschäftsführer einer juristischen Person erfasst ist. Soweit die Angaben sich auf ein Einzelunternehmen oder eine sogenannte Ein-Mann-GmbH beziehen, handelt es sich jedoch um personenbezogene Daten.

Der Schutz von Daten über juristische Personen und Personenvereinigungen bestimmt sich nach den allgemei-

nen Vorschriften, zum Beispiel nach § 5 VwVfGBbg, § 203 des Strafgesetzbuches (StGB) oder speziellen Regelungen wie zum Beispiel § 18 des Brandenburgischen Statistikgesetzes (BbgStatG).

3.3 Die natürliche Person muss bestimmt (zum Beispiel durch Identifizierungsdaten wie Name und Anschrift, Personalnummer, Kontonummer) oder bestimmbar sein (zum Beispiel durch Bezugnahme auf andere Daten oder äußere Umstände). Aggregierte Daten, wie sie zum Beispiel in der Statistik anfallen, sind nicht personenbezogen; enthält die statistische Gruppe nur Angaben über eine bis drei Personen, so sind die Daten grundsätzlich wieder als personenbezogen anzusehen. Gegebenenfalls muss die Gruppe auch noch größer gefasst sein, um eine Personenbeziehbarkeit auszuschließen.

3.4 Bei personenbezogenen Daten, bei denen die verantwortliche Stelle Namen und Anschrift der Betroffenen nicht kennt, ist sie von der Einhaltung solcher Bestimmungen entbunden, die diese Kenntnis voraussetzen.

3.5 Erheben ist das zielgerichtete (= mit Wissen und Wollen) Beschaffen oder die Entgegennahme personenbezogener Daten, und zwar auch dann, wenn der Vorgang nicht in eine Verarbeitung oder Nutzung einmündet. Beispiel: Eine Befragung ergibt, dass keine weiteren Maßnahmen zu treffen sind.

3.6 Speichern ist das Erfassen, Aufnehmen oder Aufbewahren (zum Beispiel gezielte Aneignung zum Zwecke eigener Verwendung) personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung. Datenträger ist dabei jeder Informationsträger, auf dem Daten lesbar festgehalten sind, zum Beispiel auch eine Liste oder ein einzelnes Blatt oder ein Foto beziehungsweise eine Videoaufnahme. Das Speichern endet mit dem Löschen der Daten.

3.7 Verändern beinhaltet jegliches inhaltliche Umgestalten gespeicherter Daten.

3.8 Übermitteln setzt grundsätzlich voraus, dass personenbezogene Daten zielgerichtet in den Einflussbereich eines Dritten gelangen. Auch eine unbeabsichtigte, aber tatsächlich erfolgte Übermittlung kann zielgerichtet sein. Weitergeben umfasst sowohl die physische Übergabe, Aushändigung oder Übersendung von Datenträgern als auch die bloße Informationsvermittlung (zum Beispiel fernmündlich oder durch schlüssiges Verhalten). Hierbei ist nicht erforderlich, dass der Dritte die Daten tatsächlich zur Kenntnis nimmt. Eine Übermittlung durch Einsicht oder Abruf liegt nur vor, wenn der Dritte von der verantwortlichen Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten tatsächlich einsieht oder abruft. Ein Unterfall der Übermittlung ist die Veröffentlichung. Hierbei handelt es sich um die Weitergabe von Daten an unbestimmte Dritte, zum Beispiel über Pressemitteilungen oder die Beantwortung von Presseanfragen. Das Merkmal der Veröffentlichung ist aber auch erfüllt, wenn Daten zum Abruf für unbestimmte Dritte, also für jedermann - in der Regel über das Internet - bereitgehalten werden.

3.9 Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nur noch unter eingeschränkten Voraussetzungen übermittelt oder genutzt werden (vergleiche Verwaltungsvorschriften zu § 19 BbgDSG). Die Sperrung kann bei elektronischen Daten durch die Verhinderung des Zugriffs auf die gesperrten Datenfelder oder Datensätze erfolgen. Die Verarbeitungssoftware ist so zu gestalten, dass Zugriffe erst möglich sind, wenn die gesetzlichen Voraussetzungen geprüft wurden. Bei Daten, die in Akten beziehungsweise auf Papier enthalten sind, ist ein entsprechender schriftlicher Vermerk mit Hinweis auf § 19 BbgDSG anzubringen.

3.10 Mit dem Löschen endet die Verarbeitung der Daten. Gelöscht sind personenbezogene Daten, wenn diese auch unter Zuhilfenahme technischer Mittel nicht mehr zur Kenntnis genommen werden können. Bevor personenbezogene Daten gelöscht werden, ist zu prüfen, ob diese nach den archivrechtlichen Vorschriften einem Archiv anzubieten sind (§ 19 Absatz 4 BbgDSG).

Das Löschen personenbezogener Daten kann auf verschiedene Weise geschehen. Auf Papier gespeicherte personenbezogene Daten können durch Vernichten des Datenträgers (zum Beispiel Verbrennen oder Zerkleinern unter Einhaltung der DIN-Normen im Reißwolf) gelöscht werden. Schriftzeichen auf Papier können auch durch Ausstreichen, Überschreiben oder Schwärzen unkenntlich gemacht werden. Beim Schwärzen einzelner Daten eines Datensatzes ist darauf zu achten, dass die unkenntlich zu machende Information dauerhaft nicht erhalten bleibt. Gegebenenfalls kann es notwendig sein, eine Kopie des geschwärzten Papiers zur Akte zu nehmen und das Original mechanisch zu vernichten, da unter Umständen die Information trotz der Streichung sichtbar bleibt. Auf maschinenlesbaren Datenträgern sind Daten dann unkenntlich, wenn sichergestellt ist, dass sie von niemandem mehr zur Kenntnis genommen werden können. Das kann zum Beispiel durch Überschreiben geschehen, wenn die Daten danach für den Lesekopf der Verarbeitungsanlage nicht mehr lesbar gemacht werden können. Eine Löschung kann auch durch thermische, mechanische oder chemische Verfahren erreicht werden. Daten sind erst dann vollständig gelöscht, wenn auch die Datenträger, die der Datensicherung dienen (Duplikate, Archivbänder), gelöscht wurden.

3.11 Nutzen ist jede Verwendung personenbezogener Daten, die nicht unter die vorgenannten Definitionen fällt. Das Nutzen ist ein Auffangtatbestand, der immer dann greift, wenn eine Verwendung der Daten keiner Phase der Datenverarbeitung zugeordnet werden kann. Damit wird sichergestellt, dass jeder Umgang mit personenbezogenen Daten vom Gesetz erfasst wird.

Nutzen ist insbesondere die Verwendung personenbezogener Daten innerhalb der verantwortlichen Stelle, zum Beispiel die interne Weitergabe an eine andere Organi-

sationseinheit innerhalb der gleichen öffentlichen Stelle. Die daran beteiligten Organisationseinheiten sind zueinander grundsätzlich nicht Dritte, so dass in diesem Falle keine Übermittlung vorliegt. In diesen Fällen ist § 14 Absatz 5 BbgDSG zu beachten. Eine Nutzung liegt auch vor, wenn personenbezogene Daten ohne (zielgerichtete) Erhebung erlangt und nicht sofort vernichtet werden, zum Beispiel Anzeigen personenbezogener Daten auf einem Bildschirm, sofern diese zur Kenntnis genommen werden oder die Verwendung personenbezogener Daten zu Testzwecken. Ebenso liegt eine Nutzung vor, wenn Datenbestände miteinander ver- beziehungsweise abgeglichen werden.

3.12 Die Anonymisierung bewirkt die Beseitigung des Personenbezugs der Daten, also eine „Entpersonalisierung" der Daten. Derjenige, der mit anonymisierten Daten umgeht, soll nicht mehr in der Lage sein, Einzelangaben bestimmten Personen zuzuordnen. Es wird klargestellt, dass personenbezogene Daten datenschutzrechtlich nicht nur dann anonymisiert sind, wenn ein Personenbezug überhaupt nicht mehr herstellbar ist, sondern auch dann, wenn die Zuordnung nur noch mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft möglich wäre (faktische Anonymisierung). Je sensibler die Daten sind, desto größer muss der Aufwand sein, sie zu repersonifizieren.

3.13 Pseudonymisieren ist das Verändern personenbezogener Daten durch Verwendung einer Zuordnungsfunktion derart, dass eine Zuordnung der Einzelangaben zu einer bestimmten oder bestimmbaren natürlichen Person nur durch Befugte in Kenntnis dieser Funktion möglich ist. Für Unbefugte wird die Zuordnung unmöglich oder zumindest erschwert, da sie die Funktion nicht kennen. An die Stelle identifizierbarer Daten tritt ein Pseudonym, das es ermöglicht, Daten ohne Kenntnis der Identität des Betroffenen zu nutzen. Die Pseudonymisierung von Daten sollte überwiegend dort eingesetzt werden, wo die wesentlich stärkere Maßnahme der Anonymisierung personenbezogener Daten nicht in Frage kommt. Die Pseudonymisierung kann zum Beispiel im Medizinbereich bei der Untersuchung von Materialien in Laboren zum Einsatz kommen. Ein Außenstehender (beispielsweise ein Techniker) kann die Daten keiner Person zuordnen. Ihm gegenüber wird das Arztgeheimnis gewahrt. Bei der Wahl des Pseudonyms ist darauf zu achten, dass dieses möglichst wenig Informationsgehalt aufweist.

3.14 Verschlüsseln ist das Ersetzen von Klartextbegriffen oder Zeichen mit Hilfe eines Verschlüsselungsverfahrens durch andere in der Weise, dass der Klartext von Unbefugten nur mit unverhältnismäßigem Aufwand wieder lesbar gemacht werden könnte.

3.15 Die Definition des mobilen personenbezogenen Datenträgers erfasst nicht nur intelligente Medien, insbesondere Chipkarten, sondern auch nicht intelligente Medien, zum Beispiel Magnetkarten, maschinenlesbare Ausweise oder RFID-Tags. Es wird nicht nur auf Prozesse abgestellt, die auf dem Medium ablaufen, sondern auch auf solche, die durch das Medium in anderen Datenverarbeitungssystemen ausgelöst werden. Je nach Verwendung können mittels solcher Datenträger Bewegungsprofile erstellt oder beim Einlesen des Datenträgers gespeicherte Daten anderen verfügbar gemacht werden. Um diesen Risiken für die Gewährleistung des Rechts auf informationelle Selbstbestimmung zu begegnen, ist vor dem Einsatz mobiler Datenträger eine Vorabkontrolle nach § 10a BbgDSG vorgeschrieben.

3.16 Datenverarbeitende Stellen sind die Stellen, die Daten selbst verarbeiten oder durch andere verarbeiten lassen. Datenverarbeitende Stellen sind grundsätzlich nicht die juristischen Personen des öffentlichen Rechts selbst, sondern deren Behörden und die von ihnen getragenen sonstigen öffentlichen Stellen. Nachgeordnete Bereiche einer Behörde sind Teil der Daten verarbeitenden Stelle, wenn sie nicht organisatorisch selbständig sind. Erhält eine Aufsicht führende Stelle personenbezogene Daten, wird sie insoweit selbst zur Daten verarbeitenden Stelle und darf diese Daten verarbeiten, soweit dies für die Aufgabenerfüllung, also für die Aufsicht, erforderlich ist. Eine weitergehende Verarbeitungsbefugnis besteht auf der Grundlage des § 13 Absatz 2 BbgDSG. Gegebenenfalls sind für eine weitergehende Verarbeitung Rechtsgrundlagen in Spezialgesetzen heranzuziehen.

Unter Daten verarbeitenden 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 Daten verarbeitende Stelle und nicht als Dritter. Ebenso ist der Betroffene nicht Dritter. Das Gesetz geht vom organisatorischen und nicht vom funktionalen Stellenbegriff aus; das heißt verschiedene Organisationseinheiten einer Behörde sind grundsätzlich zueinander nicht Dritte, wohl aber Empfänger. Die Einbeziehung anderer Organisationsteile der Daten verarbeitenden Stelle berücksichtigt den Beschluss des Bundesverfassungsgerichts vom 18. Dezember 1987 (NJW 1988 S. 959), wonach auch innerhalb einer Daten verarbeitenden Stelle eine aufgabenspezifische Trennung im Umgang mit personenbezogenen Daten besteht (informationelle Gewaltenteilung). Die stelleninterne Weitergabe personenbezogener Daten ist grundsätzlich keine Übermittlung, sondern ein Unterfall der Nutzung. Diese Differenzierung hat überwiegend nur eine formale Bedeutung, da die materiellen Voraussetzungen der internen Weitergabe und der Übermittlung im öffentlichen Bereich nach § 14 BbgDSG regelmäßig übereinstimmen.

3.17 Wesentliches Kriterium für eine automatisierte Datenverarbeitung ist, dass durch den gesteuerten Einsatz von Technik ohne weiteres menschliches Zutun die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten abläuft. Die Definition ist so offen formuliert, dass sie auch künftigen technischen Entwicklungen gerecht wird. Es kommt nicht auf die Speicherung in einer einzelnen Datei an. Entscheidend ist auch nicht, wie viele personenbezogene Daten oder Merkmale erhoben, verarbeitet oder genutzt werden. Regelungsgegenstand

sind Vorgänge oder Vorgangsreihen; diese sind mit dem Begriff Verfahren umschrieben. Grundsätzlich ist von dem Begriff jegliche IT-Software erfasst, die die Verarbeitung personenbezogener Daten erlaubt beziehungsweise dazu genutzt wird, hierzu gehören auch handelsübliche Schreibprogramme. Des Weiteren sind beispielsweise erfasst automatische Zugangssysteme zu Räumen oder Gebäuden, soweit hiermit personenbezogene Daten verarbeitet werden, aber auch die digitale Videoüberwachung ist ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten.

3.18 Das Brandenburgische Datenschutzgesetz verwendet einen doppelten Dateibegriff. Es unterscheidet zwischen automatisierten und nicht-automatisierten Dateien:

Automatisierte Dateien sind sämtliche elektronisch verarbeiteten Datenbestände personenbezogenen Inhalts, die automatisiert ausgewertet werden können. Von dem Begriff erfasst werden auch Bild- und Tonaufzeichnungen in digitalisierter Form, bei denen eine Auswertbarkeit durch automatisierte Verfahren gegeben ist.

Nicht-automatisierte Datei ist jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen (mindestens zwei) geordnet, umgeordnet und ausgewertet werden kann (zum Beispiel Kartei, Register, Sammlung von ausgefüllten Antragsvordrucken; nicht aber eine Liste, da sie - ohne physische Veränderung - nicht umgeordnet werden kann). Gleichartig aufgebaut ist eine Sammlung von Daten, die sich entweder auf einem einzigen Datenträger oder auf mehreren physisch gleichartigen Datenträgern (zum Beispiel Karteikarten) befindet. Die darauf gespeicherten Daten müssen auf dem Datenträger in einer bestimmten Ordnung enthalten sein, also in einer für die weitere Verarbeitung geeigneten Weise formalisiert sein.

Der Dateibegriff hat bei Anwendung des Gesetzes nur geringe Bedeutung. Das Brandenburgische Datenschutzgesetz regelt die materielle Zulässigkeit des Umgangs öffentlicher Stellen mit personenbezogenen Daten grundsätzlich unabhängig davon, ob automatisierte Verfahren eingesetzt werden oder ob die Daten in nicht-automatisierten Dateien oder Akten enthalten sind. Der Dateibegriff ist nur bei der Anwendung einzelner Regelungen des Brandenburgischen Datenschutzgesetzes bedeutsam, insbesondere bei solchen verfahrensrechtlicher Art. Darüber hinaus stellen andere Gesetze auf den Dateibegriff ab, so zum Beispiel das Brandenburgische Polizeigesetz (BbgPolG, siehe unter anderem § 39 Absatz 1 BbgPolG).

3.19 Der Anwendungsbereich des Brandenburgischen Datenschutzgesetzes ist weder auf den Umgang mit personenbezogenen Daten in automatisierten Verfahren noch in oder aus nicht-automatisierten Dateien beschränkt. Aus diesem Grund kommt der Definition der Akte Bedeutung zu. Das Gesetz trifft für Akten einzelne differenzierende Regelungen, die auf die Besonderheiten dieses Mediums abstellen (siehe zum Beispiel § 18 Absatz 2 BbgDSG). Akte ist abweichend vom allgemeinen Sprachgebrauch jede sonstige amtlichen, dienstlichen oder Geschäftszwecken dienende Unterlage, die nicht Datei ist. Bild- und Tonträger (zum Beispiel Fotos, Kassetten, CD's, DVD's) sind danach Akten, sofern sie nicht bereits als nicht-automatisierte Dateien einzustufen sind oder Teil eines automatisierten Verfahrens sind. Allerdings können aufgrund der technischen Entwicklung beispielsweise durch die Einführung von Bilderkennungssoftware Akten im Sinne des § 3 Absatz 7 BbgDSG zu Dateien im Sinne des § 3 Absatz 6 BbgDSG werden. Nicht vom Aktenbegriff erfasst werden Notizen und Vorentwürfe, die spätestens nach Abschluss des Verfahrens beziehungsweise des Vorgangs vernichtet werden. Welche Unterlagen Aktenbestandteil sind, richtet sich nach den Regeln für die ordnungsgemäße Aktenführung. Die Sonderregelungen für Akten und Aktensammlungen gelten nicht, soweit diese durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

4 Zu § 4 Zulässigkeit der Datenverarbeitung

4.1 Entsprechend des in Artikel 11 Absatz 1 der Landesverfassung Brandenburg (Landesverfassung) formulierten Primats der Einwilligung ist diese als Rechtfertigungsgrund für eine Datenverarbeitung den gesetzlichen Bestimmungen vorangestellt. Grundsätzlich bedarf es aber für die Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung einer gesetzlichen Grundlage. Der Staat darf seine Handlungsbefugnisse insbesondere im Bereich der Leistungs- oder Eingriffsverwaltung nicht auf der Grundlage einer Einwilligung ausweiten.

4.2 Der Begriff der freiwilligen und ausdrücklichen Zustimmung greift die Formulierung von Artikel 11 Landesverfassung auf. Eine wirksame Einwilligung setzt neben der tatsächlichen Freiwilligkeit voraus, dass insbesondere der Zweck der Verarbeitung und gegebenenfalls beabsichtigten Übermittlungen Bestandteil der Einwilligungserklärung sind. Der Umfang der Ermächtigung zur Datenverarbeitung ergibt sich grundsätzlich aus den Festlegungen in der Einwilligungserklärung. Ausnahmen hiervon sind lediglich die aus überwiegendem Allgemeininteresse vorgesehenen speziellen Vorschriften über die zweckändernde Verarbeitung erhobener oder gespeicherter Daten nach § 13 Absatz 2 BbgDSG. Ein Rückgriff auf § 13 Absatz 2 BbgDSG ist jedoch nicht möglich, wenn in der Einwilligungserklärung explizit eine Datenverarbeitung zu anderen Zwecken ausgeschlossen ist.

4.3 Eine Einwilligung kommt nur in den Bereichen in Betracht, die keiner Regelung durch Rechtsvorschriften unterliegen. Gesetze oder Rechtsvorschriften im Sinne von § 4 Absatz 1 Nummer 2 BbgDSG sind materielle Rechtsnormen im weitesten Sinne, zum Beispiel auch kommunale Satzungen und Satzungen sonstiger öffentlich-rechtlicher Körperschaften (zum Beispiel der IHK).

4.4 Die Einwilligung zur Verarbeitung personenbezogener Daten gemäß § 4 Absatz 1 Nummer 1 BbgDSG kann

nach Absatz 3 auch elektronisch erklärt werden. Diese Regelung entspricht den modernen datenschutzrechtlichen Regelungen im Multimediabereich, die der Bund und die Länder übereinstimmend getroffen haben. Auch im allgemeinen Datenschutzrecht soll die Möglichkeit einer elektronischen Einwilligungserklärung gegeben sein. Die Anforderungen des § 4 Absatz 3 BbgDSG an die elektronische Einwilligung verlangen die Verwendung einer qualifizierten elektronischen Signatur entsprechend dem Signaturgesetz. Überall da, wo Rechtsvorschriften die datenschutzrechtliche Einwilligung vorschreiben, gelten hierfür die Voraussetzungen des § 4 Absatz 3 BbgDSG.

4.5 Für die Vorschriften des Brandenburgischen Datenschutzgesetzes, die ansonsten die Schriftform anordnen, (unter anderem § 4b, § 7 Absatz 3, § 11 Absatz 2, § 18 Absatz 2, § 23 Absatz 5 BbgDSG) bewirkt die Regelung des § 3a VwVfG, dass das schriftliche Dokument im herkömmlichen Sinne durch das elektronische Dokument mit qualifizierter elektronischer Signatur ersetzt werden kann.

4.6 In § 4 Absatz 4 BbgDSG wird die in Artikel 15 der EG-Datenschutzrichtlinie[1] enthaltene Regelung zum Verbot automatisierter Einzelentscheidungen umgesetzt. Entscheidungen, die auf einer Bewertung des Betroffenen beruhen, und damit sein Persönlichkeitsrecht im Kern berühren, dürfen nicht allein einer technischen Vorrichtung überlassen werden, sondern müssen letztlich immer von einem Menschen verantwortet werden. Eine Ausnahme ist nur durch besonderes Gesetz zulässig, das die Wahrung des berechtigten Interesses des Betroffenen sicherstellt.

4.7 Das Verbot der automatisierten Einzelentscheidung kommt dann zum Tragen, wenn mehrere Informationen über die Persönlichkeit der betroffenen Person zusammengeführt werden und einer rein automatisierten Bewertung unterzogen werden sollen. Die ausgewerteten Informationen müssen dabei eine gewisse Komplexität (zum Beispiel Angaben über die berufliche Leistung, die Zuverlässigkeit) aufweisen. Nicht erlaubt ist beispielsweise die Beurteilung von Beschäftigten allein auf der Grundlage von Informationen, die aus einer automatisierten Verarbeitung gewonnen wurden. Bloße Vorentscheidungen, wie etwa die automatisierte Vorauswahl im Vorfeld einer Personalbesetzung (automatisierter Abgleich des Personalbestandes anhand bestimmter Suchkriterien wie Ausbildung, Zusatzqualifikation) sind von dem Verbot nicht erfasst.

5 Zu § 4a Verarbeitung besonderer Kategorien personenbezogener Daten

5.1 Die Verarbeitung besonderer Kategorien personenbezogener Daten darf nur auf der Grundlage spezieller Rechtsvorschriften erfolgen. Diese müssen die Verarbeitung ausdrücklich regeln oder zwingend voraussetzen.

5.2 Für alle anderen Fälle bestimmt die Vorschrift entsprechend Artikel 8 Absatz 2 der EG-Datenschutzrichtlinie abschließend die Voraussetzungen, unter denen diese Daten verarbeitet werden dürfen:

a) Zum einen ist die Datenverarbeitung auf der Grundlage der Einwilligung des Betroffenen zulässig. Die Einwilligung muss sich dabei ausdrücklich auf die jeweils zu verarbeitenden besonderen Kategorien personenbezogener Daten beziehen. Darüber hinaus gelten hinsichtlich der Einwilligungserklärung die übrigen Voraussetzungen von § 4 Absatz 2 und 3 BbgDSG.

b) Neben der Einwilligung ist die Verarbeitung zum anderen auf der Grundlage einzelner Regelungen des Brandenburgischen Datenschutzgesetzes zulässig. Dies betrifft die Verarbeitung (sensibler) Daten für wissenschaftliche Zwecke (§ 28 BbgDSG), in Dienst- und Arbeitsverhältnissen (§ 29 BbgDSG), durch Religionsgesellschaften (§ 15 BbgDSG), durch den Landtag (§ 31 BbgDSG), für öffentliche Auszeichnungen und Ehrungen (§ 33a BbgDSG), in Begnadigungsverfahren (§ 33b BbgDSG) sowie bei der Videoüberwachung und -aufzeichnung (§ 33c BbgDSG).

5.3 Eine Verarbeitung ist entsprechend Artikel 8 der EG-Datenschutzrichtlinie auch zulässig, wenn der Betroffene diese Daten offenkundig selbst öffentlich gemacht hat. Sollen solche Daten verarbeitet werden, obliegt der öffentlichen Stelle eine besondere Sorgfaltspflicht bei der Prüfung, ob die Daten von dem Betroffenen offenkundig selbst öffentlich gemacht wurden. Öffentlich gemacht hat der Betroffene seine Daten beispielsweise dann, wenn er diese veröffentlicht (zum Beispiel in wissenschaftlichen Aufsätzen oder literarisch publiziert) oder wissentlich in der Öffentlichkeit gegenüber einem unbestimmten Personenkreis, zu dem potenziell jedermann gehören kann (zum Beispiel auf Versammlungen, im Fernsehen oder im Internet), kundgibt. Die Preisgabe gegenüber einem beschränkten Personenkreis (zum Beispiel auf geschlossenen, nicht-öffentlichen Veranstaltungen oder innerhalb geschlossener Benutzergruppen im Internet) reicht nicht aus. Bestehen Zweifel daran, dass der Betroffene seine Daten selbst öffentlich bekannt gemacht hat, ist die Verarbeitung der Daten nur zulässig, soweit die dafür in § 4a Satz 1 und 2 BbgDSG bestimmten Voraussetzungen vorliegen.

6 Zu § 4b Widerspruchsrecht des Betroffenen aus besonderem Grund

6.1 Diese Vorschrift entspricht Artikel 14 der EG-Datenschutzrichtlinie. Danach hat der Betroffene ein Widerspruchsrecht gegen die Verarbeitung seiner Daten, wenn ihr überwiegende schutzwürdige Gründe entgegenstehen. Dies gilt auch, wenn die Daten Gegenstand einer rechtmäßigen Verarbeitung auf Grund eines öffentlichen Interesses oder der Ausübung hoheitlicher Gewalt sind.

[1] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbietung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31)

6.2 Das Widerspruchsrecht darf nicht mit der Möglichkeit des Betroffenen, Verwaltungsakte im verwaltungsgerichtlichen Vorverfahren anzufechten, verwechselt werden. Vielmehr kann der Betroffene mit schriftlichem Antrag ein Verfahren einleiten, in dem seine schutzwürdigen besonderen persönlichen Interessen mit dem öffentlichen Interesse an der Datenverarbeitung im Einzelfall abzuwägen sind und das mit der Erteilung eines Bescheides über die Zulässigkeit der Datenverarbeitung abgeschlossen wird. Gelangt die Behörde bei der Abwägung zu dem Ergebnis, dass die von dem Betroffenen vorgetragenen persönlichen Gründe das öffentliche Interesse an der Verarbeitung der Daten überwiegen, dann muss diese unterbleiben oder so gestaltet werden, wie es dem Anliegen des Betroffenen entspricht. Die Einwendung kann zum Beispiel darauf gerichtet sein, dass eine Angelegenheit, die höchstpersönliche Daten zum Gegenstand hat, nicht von zum Bekanntenkreis der betroffenen Person gehörenden Mitarbeitern bearbeitet wird. Solche Personen sind nicht zwingend nach § 20 VwVfG in Verbindung mit § 3 VwVfGBbg vom Handeln ausgeschlossen.

6.3 Das Ergebnis der Abwägung ist den Betroffenen mitzuteilen. Gegen eine ablehnende Entscheidung kann nach den Regeln des Verwaltungsprozessrechtes Widerspruch eingelegt oder Klage erhoben werden (§§ 68 bis 70 der Verwaltungsgerichtsordnung - VwGO).

7 Zu § 7 Sicherstellung des Datenschutzes

7.1 § 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 Absatz 1 BbgDSG genannten öffentlichen Stellen und verpflichtet sie, für ihren Bereich die Ausführung aller Datenschutzvorschriften sicherzustellen.

7.2 Dabei ist die Datenverarbeitung an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten (Grundsatz der Datensparsamkeit). Ebenso ist zu beachten, dass eine Trennung nach Betroffenen und Zwecken der Datenverarbeitung gewährleistet wird.

7.3 Die angesprochenen öffentlichen Stellen haben unter anderem dafür zu sorgen, dass die in Datenschutzvorschriften enthaltenen Verbote beachtet, Datenschutzpflichten erfüllt und die notwendigen Datensicherungsmaßnahmen getroffen und eingehalten werden. Orientierungshilfen für eine diesbezügliche Prüfung können sich aus Empfehlungen und/oder Checklisten ergeben, die von den Datenschutzbeauftragten des Bundes und der Länder veröffentlicht werden.

7.4 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 beispielsweise das Sicherstellen, dass Programme nur zu vorgesehenen Zwecken eingesetzt werden. Des Weiteren zählt dazu, dass das Personal, das mit der Verarbeitung personenbezogener Daten betraut werden soll, zur fachgerechten Anwendung der Datenverarbeitungsprogramme befähigt wird.

7.5 Die Art und Weise der Ausführung der Datenschutzvorschriften bleibt den Normadressaten überlassen, damit den Besonderheiten der verschiedenen Verwaltungszweige Rechnung getragen werden kann.

7.6 Soweit die Adressaten des Brandenburgischen Datenschutzgesetzes beabsichtigen, Rechts- oder Verwaltungsvorschriften zu erlassen, die die Verarbeitung personenbezogener Daten betreffen, ist der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht (LDA) vorab zu beteiligen. Dies betrifft Vorschriften, die die Verarbeitung personenbezogener Daten sowohl durch öffentliche Stellen als auch durch nicht-öffentliche Stellen regeln. Mit umfasst sind auch solche Rechtsvorschriften, die von den Gemeinden oder Gemeindeverbänden erlassen werden, wie beispielsweise Satzungen.

7.7 Der LDA ist darüber hinaus über Planungen des Landes zum Aufbau oder zur wesentlichen Änderung automatisierter Systeme, mit denen personenbezogene Daten verarbeitet werden zu unterrichten. Als automatisierte Informationssysteme sind Verfahren insbesondere dann anzusehen, wenn sie landesweit oder ressortübergreifend zur Anwendung kommen (zum Beispiel Personalverwaltungs-, Dokumentenmanagementsysteme oder Systeme zur gemeinsamen Bearbeitung bestimmter Verwaltungsaufgaben). Gleiches gilt für ressortspezifische Anwendungen, wenn sehr große Datenmengen beziehungsweise die Daten einer Vielzahl von Personen verarbeitet werden (zum Beispiel bei zu Übermittlungszwecken geführten Registern). Erfasst werden auch Planungen zur Gestaltung der technischen Infrastruktur, wie zum Beispiel die E-Government-Strategie des Landes, soweit es um die Prüfung der Erforderlichkeit oder die Realisierung technischer und organisatorischer Maßnahmen zur Gewährleistung der Sicherheitsziele des § 10 BbgDSG im Allgemeinen geht. Der LDA ist rechtzeitig und mit einer angemessenen Frist zu beteiligen.

7.8 Bevor ein automatisiertes Verfahren zur Verarbeitung personenbezogener Daten (vergleiche Nummer 3.17) zum ersten Mal zum Einsatz gebracht wird, bedarf es, wenn ein Verfahrensverzeichnis nach § 8 BbgDSG zu erstellen ist, der schriftlichen Freigabe. Das heißt, das entsprechende Verfahren darf erst dann in Betrieb gehen, wenn es durch die Daten verarbeitende Stelle förmlich freigegeben wurde.

Mit der Verpflichtung zur Durchführung eines Freigabeverfahrens und der damit verbundenen Vorabüberprü-

fung eines Verfahrens soll erreicht werden, dass nur solche Verfahren zum Einsatz kommen, die die datenschutzrechtlichen Bedingungen in vollem Umfang erfüllen. Die Beteiligung des behördlichen Datenschutzbeauftragten sollte bereits zu Beginn der Programmentwicklung erfolgen, damit nicht später unter Umständen sehr kostenintensive Nachbesserungen an Programmen vorgenommen werden müssen.

7.9 Die Freigabe darf nur erfolgen, wenn ein aus einer Risikoanalyse entwickeltes Sicherheitskonzept (das zum Beispiel entsprechend den methodischen Empfehlungen und Standards des BSI, gegebenenfalls aber auch nach anderen Kriterien erstellt werden kann) ergeben hat, dass die von dem Verfahren ausgehenden Risiken für die Rechte und Freiheiten der Betroffenen durch entsprechende technisch-organisatorische Maßnahmen nach § 10 Absatz 1 und 2 BbgDSG beherrscht werden können und, sofern erforderlich, eine Vorabkontrolle nach § 10a BbgDSG erfolgt ist.

7.10 Ausgangspunkt des Freigabeverfahrens und Basis des Sicherheitskonzepts ist die Risikoanalyse. Hierbei ist ausgehend von den konkret zu verarbeitenden personenbezogenen Daten zu untersuchen, ob und wenn ja, welche Risiken für die Rechte der Betroffenen von dem geplanten Verfahren ausgehen können.

7.11 Im Sicherheitskonzept ist darzustellen, wie diese Risiken durch technisch-organisatorische Maßnahmen nach § 10 BbgDSG beherrscht werden können. Tiefe und Umfang des Sicherheitskonzepts orientieren sich an den spezifischen Risiken, die von einem Verfahren ausgehen und an der bereits in einer Daten verarbeitenden Stelle existierenden Sicherheitsarchitektur. Das Sicherheitskonzept ist entsprechend der technischen Entwicklung in angemessenen Abständen fortzuschreiben. Eine Fortschreibung ist darüber hinaus erforderlich, wenn sich die Gegebenheiten vor Ort ändern oder geändert haben, beispielsweise nach einem Umzug.

7.12 Im Rahmen der Freigabe ist auch zu überprüfen, ob die vorgesehene Verarbeitung der Daten datenschutzrechtlich zulässig ist (§ 4 BbgDSG), ob das Programm den vorgesehenen Zweck erfüllt und ob der Grundsatz der Datenvermeidung und Datensparsamkeit berücksichtigt wurde.

7.13 Ein Freigabeverfahren ist auch dann durchzuführen, wenn in einem bereits freigegebenen Verfahren wesentliche Änderungen durchgeführt werden. Wesentlich sind Änderungen dann, wenn sich die dem Verfahrensverzeichnis zugrunde liegenden Sachverhalte erheblich geändert haben. Solche Änderungen können beispielsweise Programmänderungen oder -erweiterungen sein, bei denen neue beziehungsweise modifizierte Dateien entstehen oder die Umstellung einer Verarbeitung auf eine neue Software, Outsourcing oder die Einbeziehung neuer Kategorien personenbezogener Daten beziehungsweise Betroffener erfolgt.

7.14 Welche Organisationseinheit innerhalb einer Daten verarbeitenden Stelle die Freigabe erklärt, unterliegt der Organisationshoheit der jeweiligen Daten verarbeitenden Stelle. Dies ist in der Regel die Organisationseinheit, die die fachliche Verantwortung für die (materielle) Rechtmäßigkeit des Verfahrens trägt. Aufgrund der Komplexität der nach § 10 BbgDSG zu treffenden technischen Maßnahmen kann die Freigabe - gegebenenfalls nach Bestätigung der materiellen Rechtmäßigkeit durch die fachlich zuständige Organisationseinheit - aber auch durch die für die IT zuständige Organisationseinheit oder den Leiter der Daten verarbeitenden Stelle erfolgen. In jedem Falle ist die Fachebene und gegebenenfalls der Geheimschutzbeauftragte in das Freigabeverfahren einzubeziehen. Der behördliche Datenschutzbeauftragte soll beim Freigabeverfahren beratend mitwirken.

7.15 Bei gemeinsam betriebenen Verfahren erfolgt eine Freigabe durch die in der Vereinbarung nach § 9 Absatz 1a Satz 1 BbgDSG bestimmte Stelle beziehungsweise Stellen. Die in der Vereinbarung festgelegte Abgrenzung der Verantwortlichkeiten schließt auch die Freigabe für die dem jeweiligen Verantwortungsbereich unterfallenden Komponenten ein. In der Freigabeerklärung ist auf der Basis der Vereinbarung nach § 9 Absatz 1a BbgDSG der Bereich, auf den sich die Freigabe bezieht, zu definieren.

8 Zu § 7a Behördlicher Datenschutzbeauftragter

8.1 Alle Daten verarbeitenden Stellen im Sinne des § 2 Absatz 1 BbgDSG haben einen behördlichen Datenschutzbeauftragten zu bestellen. Mit der Funktion dürfen nur Personen betraut werden, die über die technischen, rechtlichen und organisatorischen Kenntnisse verfügen, die sie, abhängig von den Gegebenheiten der öffentlichen Stelle, in die Lage versetzen, ihre Aufgabe wahrzunehmen. Die Anforderungen an die Fachkunde sind nicht einheitlich definiert, sondern hängen unter anderem von der Größe der öffentlichen Stelle, der Sensibilität der verarbeiteten personenbezogenen Daten und der eingesetzten Technik ab. Gefordert sind mindestens Grundkenntnisse über Verfahren und Techniken der automatischen Datenverarbeitung, allgemeine juristische Kenntnisse, Kenntnisse des Datenschutzrechts und sonstiger relevanter Vorschriften sowie ausreichende Kenntnisse der Verwaltungsorganisation und -aufgaben.

8.2 Der Beauftragte für den Datenschutz muss die Möglichkeit erhalten, die notwendigen Kenntnisse durch geeignete Fortbildungsangebote zu erwerben beziehungsweise zu erweitern.

8.3 Im Rahmen der Prüfung der Zuverlässigkeit des behördlichen Datenschutzbeauftragten ist sicherzustellen, dass mit dieser Funktion nur ein Bediensteter betraut wird, der dadurch nicht in einen Interessenkonflikt mit seinen regelmäßig wahrzunehmenden sonstigen Aufgaben gerät. Ein Interessenkonflikt ist dann anzunehmen, wenn der Betroffene hauptverantwortlich für Bereiche ist, die der Kontrolle des behördlichen Datenschutzbeauftrag-

ten unterliegen. Dies wäre beispielsweise bei leitenden Mitarbeitern der Personalstelle, der für die IT zuständigen Organisationseinheit oder bei sonstigen Stellen, deren Hauptaufgabe in der Verarbeitung personenbezogener Daten besteht, der Fall. Darüber hinaus ist zu gewährleisten, dass der behördliche Datenschutzbeauftragte mit den notwendigen Ressourcen ausgestattet ist. Dies betrifft sowohl die materielle Ausstattung als auch den für diese Tätigkeit zur Verfügung stehenden Zeitanteil. Letzterer richtet sich vor allem nach den genutzten Verfahren zur Verarbeitung personenbezogener Daten. Es muss gewährleistet sein, dass der behördliche Datenschutzbeauftragte seinen Verpflichtungen im ausreichenden Umfang nachkommen kann.

8.4 Die Bestellung eines behördlichen Datenschutzbeauftragten kann nur in entsprechender Anwendung des § 626 BGB, der die fristlose Kündigung eines Dienstvertrages aus wichtigem Grund regelt, widerrufen werden (§ 7a Absatz 1 Satz 3 BbgDSG). Mit dieser Regelung wird verhindert, dass eine Daten verarbeitende Stelle ohne triftigen Grund einen behördlichen Datenschutzbeauftragten gegen dessen Willen abberuft. Sie stärkt die Unabhängigkeit der Datenschutzbeauftragten. Im Interesse der Daten verarbeitenden Stellen an einem flexiblen Personaleinsatz ist es möglich, den behördlichen Datenschutzbeauftragten zeitlich befristet zu bestellen. Dies ist jedoch nur zulässig, wenn hierdurch nicht seine Unabhängigkeit gefährdet wird. Gemäß der Gesetzesbegründung entspricht eine Befristung dieser Anforderung, wenn die Bestellung mindestens für fünf Jahre erfolgt.

8.5 Absatz 2 eröffnet die Möglichkeit, dass ein Bediensteter einer anderen Daten verarbeitenden Stelle zum behördlichen Datenschutzbeauftragten bestellt werden kann. So können zum Beispiel mehrere kleine Gemeinden einen gemeinsamen Datenschutzbeauftragten bestellen. Es ist jedoch nicht zugelassen, eine Person außerhalb des öffentlichen Bereichs mit der Aufgabe eines Datenschutzbeauftragten zu betrauen.

8.6 Der Beauftragte für den Datenschutz ist in dieser Funktion, also insbesondere bei Wahrnehmung seiner Beratungs- und Kontrolltätigkeit, weisungsfrei. Die Weisungsfreiheit entbindet Beauftragte für den Datenschutz jedoch nicht davon, nach Recht und Gesetz zu handeln, zum Beispiel bei der Auskunftserteilung gegenüber Betroffenen.

8.7 Absatz 3 Satz 3 sichert die Unabhängigkeit durch ein ausdrückliches Benachteiligungsverbot. Dadurch sind Beauftragte für den Datenschutz vor Umsetzungen, Kündigungen oder anderen Beeinträchtigungen geschützt, die aus einer nicht genehmen Wahrnehmung ihrer Funktion als Beauftragte für den Datenschutz herrühren könnten. Ob eine Benachteiligung vorliegt, kann gerichtlich überprüft werden.

8.8 Beauftragte für den Datenschutz sollten in den Organigrammen der öffentlichen Stellen gesondert ausgewiesen werden. Die besondere Stellung des Beauftragten für den Datenschutz wird dadurch deutlich, dass er sich unmittelbar an die Leitung der öffentlichen Stellen wenden kann.

8.9 Der Beauftragte für den Datenschutz kann sich in Zweifelsfällen unmittelbar an den LDA wenden.

8.10 In Absatz 5 werden die Aufgaben des behördlichen Datenschutzbeauftragten exemplarisch aufgeführt:

a) Hinwirken auf die Beachtung datenschutzrechtlicher Vorschriften umfasst zum Beispiel

   aa) die Prüfung der datenschutzrechtlichen Zulässigkeit von Verfahren, über deren Einsatz öffentliche Stellen entscheiden. Hierzu ist er über Vorhaben zur automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.
   bb) die Prüfung von Dienstanweisungen und Dienstvereinbarungen zum Umgang mit personenbezogenen Daten der Beschäftigten,
   cc) die Prüfung, ob die Individualrechte Betroffener auf Benachrichtigung, Auskunft, Berichtigung, Löschung und Sperrung beachtet werden und
   dd) die Unterbreitung von Hinweisen und Vorschlägen zur Datenvermeidung und Datensparsamkeit und zur Verbesserung technischer und organisatorischer Maßnahmen gemäß § 10 BbgDSG.

b) Der behördliche Datenschutzbeauftragte hat die mit der Verarbeitung personenbezogener Daten beschäftigten Personen mit den einschlägigen datenschutzrechtlichen Vorschriften vertraut zu machen. Hierzu kann er Mitarbeiterschulungen vornehmen, soweit solche nicht im Rahmen der zentralen Mitarbeiterfortbildung erfolgen.

c) Der behördliche Datenschutzbeauftragte ist verpflichtet, die öffentlichen Stellen bei der Ausführung der Vorschriften des Brandenburgischen Datenschutzgesetzes und anderer datenschutzrechtlicher Vorschriften zu unterstützen. Die Verantwortlichkeit für den Datenschutz liegt unverändert bei den verantwortlichen öffentlichen Stellen. Der behördliche Datenschutzbeauftragte hat dementsprechend keine Weisungsbefugnisse innerhalb der öffentlichen Stellen. In welchem Umfang die Unterstützung der Daten verarbeitenden Stelle durch den behördlichen Datenschutzbeauftragten bei der Erarbeitung von Risikoanalyse und Sicherheitskonzept nach § 7 Absatz 3 BbgDSG erfolgt, bleibt der Organisationsentscheidung der jeweiligen Daten verarbeitenden Stelle vorbehalten. Er ist jedoch in jedem Fall einzubeziehen. Die Beteiligung sollte möglichst frühzeitig geschehen.

d) Der behördliche Datenschutzbeauftragte führt gemäß § 8 Absatz 2 BbgDSG das Verfahrensverzeich-

nis. Mithin erteilt er hieraus auch Auskünfte nach § 8 Absatz 4 BbgDSG an Interessierte.

e) Im Hinblick auf das Urteil des Bundesarbeitsgerichts vom 29. Oktober 1997 (NJW 1998 S. 2466) kann vereinbart werden, dass Verfahren der jeweiligen Personalvertretungen nicht in das vom behördlichen Datenschutzbeauftragten geführte Verfahrensverzeichnis aufgenommen werden. Ungeachtet dessen hat der behördliche Datenschutzbeauftragte ein uneingeschränktes Kontrollrecht beim Personalrat (§ 94 Absatz 1 des Personalvertretungsgesetzes für das Land Brandenburg).

f) Behördliche Datenschutzbeauftragte haben die Vorabkontrolle nach § 10a BbgDSG durchzuführen.

g) Durch die Regelung des § 7a Absatz 5 Satz 4 BbgDSG wird eine effektive Aufgabenerfüllung dadurch abgesichert, dass dem behördlichen Datenschutzbeauftragten bei der Kontrolle weder das Personalakten- noch das Arztgeheimnis entgegengehalten werden können. Ebenso ist eine Überprüfung nicht von der Einwilligung der Betroffenen abhängig.

9 Zu § 8 Verfahrensverzeichnis

9.1 Jede Stelle, die personenbezogene Daten selbst automatisiert verarbeitet oder im Auftrag verarbeiten lässt, hat Verzeichnisse über die dabei angewandten Verfahren zu führen, soweit nicht die Ausnahmetatbestände von § 8 Absatz 5 BbgDSG vorliegen. Beim Anlegen der Verzeichnisse sind die Verordnung zum Verfahrensverzeichnis (VerfVerzV) und die hierzu ergangenen Hinweise des Ministeriums des Innern vom 14. Oktober 2009 zu beachten (Anlage 1).

9.2 Die Verzeichnisse sollten von den fachlich zuständigen Stellen, gegebenenfalls mit Unterstützung beziehungsweise Beratung des behördlichen Datenschutzbeauftragten und des IT-Sicherheitsbeauftragten erarbeitet werden.

9.3 Der behördliche Datenschutzbeauftragte führt die Verfahrensverzeichnisse. Dies bedeutet, dass er die Verfahrensverzeichnisse einer Daten verarbeitenden Stelle sammelt und zur Einsichtnahme bereithält. Die Verfahrensverzeichnisse sind ihm daher spätestens unverzüglich nach Beginn der Datenverarbeitung beziehungsweise nach einer wesentlichen Änderung eines Verfahrens zuzuleiten.

10 Zu § 9 Gemeinsame Verfahren, automatisiertes Abrufverfahren und regelmäßige Datenübermittlung

10.1 Gemeinsame Verfahren sind solche Verfahren, die von mehreren Stellen genutzt werden, um personenbezogene Daten in oder aus einem gemeinsamen Datenbestand zu verarbeiten. Maßgeblich ist die Nutzung eines gemeinsamen Datenbestandes, zum Beispiel einer Datenbank. Werden lediglich einheitliche Programme eingesetzt, bei denen jedoch keine gemeinsame Datenbank genutzt wird, liegt kein gemeinsames Verfahren vor. Keine gemeinsamen Verfahren sind daher beispielsweise Verfahren, bei denen die beteiligten Stellen zwar die gleiche Software nutzen und gegebenenfalls die Datenverarbeitung im Wege der Auftragsdatenverarbeitung beim gleichen Auftragnehmer durchführen lassen, aber die jeweiligen Datenverarbeitungen in getrennten Datenbanken ablaufen.

10.2 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 Datensicherheit besondere Bedeutung zu. Die abrufende Stelle erhält durch den Anschluss die Möglichkeit, über bestimmte Datenbestände der Daten verarbeitenden Stelle zu verfügen.

10.3 Vor der Einrichtung gemeinsamer oder automatisierter (Abruf-)Verfahren ist eine Prüfung vorzunehmen, ob dies unter Beachtung der Rechte der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Einrichtung solcher Verfahren auf der Grundlage von § 9 BbgDSG kommt nur dann in Betracht, wenn etwaige Risiken für die Rechte der Betroffenen nicht bestehen oder durch technische und organisatorische Maßnahmen abgesichert werden können. Wegen der besonderen Risiken unterliegen diese Verfahren der Vorabkontrolle durch den behördlichen Datenschutzbeauftragten nach § 10a BbgDSG. Sofern sich im Rahmen der Prüfung nach Absatz 1 oder § 10a BbgDSG herausstellt, dass sich das Risiko unrechtmäßiger Datenabrufe nicht beherrschen lässt, ist die Einrichtung unzulässig.

10.4 Der LDA ist rechtzeitig und mit angemessener Frist für eine Bewertung vor der Einrichtung eines gemeinsamen Verfahrens oder eines automatisierten Abrufverfahrens zu unterrichten.

10.5 In Absatz 1a Satz 1 wird bestimmt, dass die an einem gemeinsamen Verfahren beteiligten Stellen die Aufgaben klar abzugrenzen haben. Hierdurch soll erreicht werden, dass für jede beteiligte Stelle Klarheit über die Verantwortlichkeiten besteht und bei Verstößen gegen datenschutzrechtliche Vorschriften die verantwortliche Stelle identifiziert werden kann. Absatz 1a Satz 2 soll weitestgehende Transparenz für das gesamte Verfahren gewährleisten. Hierzu sind die Verfahrensverzeichnisse aller beteiligten Stellen bei der für das Verfahren insgesamt zuständigen Stelle zusammenzuführen und dort zur Einsicht gemäß § 8 Absatz 4 BbgDSG bereit zu halten.

10.6 Die Regelung von Absatz 1b dient der Durchsetzung der Rechte der Betroffenen. Diese können sich an jede der beteiligten Stellen wenden, welche das Anliegen an die im Einzelfall verantwortliche Stelle weiterzuleiten haben.

10.7 Die in Absatz 2 Nummer 1 bis 4 genannten Angaben ergänzen beziehungsweise konkretisieren § 10 BbgDSG. Ihre Dokumentation erfolgt zu Kontrollzwecken zusätzlich zu den nach § 8 BbgDSG im Verfahrensverzeichnis verzeichneten Angaben. Die Gesamtheit der in Absatz 2 genannten Aspekte sind in die Überlegungen hinsichtlich der Angemessenheit nach Absatz 1 einzubeziehen. Durch die Verpflichtung zur Dokumentation dieser Angaben wird insbesondere die Selbstkontrolle der speichernden Stelle unterstützt. Die Angaben dienen aber auch als Grundlage einer externen Kontrolle durch den LDA beziehungsweise gegebenenfalls der Aufsichtsbehörde. Daneben besteht für die an einem Abrufverfahren beteiligten Stellen die Verpflichtung, jeweils für ihren Bereich die nach § 10 BbgDSG erforderlichen Maßnahmen zu treffen, das Verfahren gemäß § 7 Absatz 3 in Verbindung mit § 10a BbgDSG freizugeben und ein Verfahrensverzeichnis nach § 8 BbgDSG zu erstellen.

10.8 Absatz 2 Satz 2 eröffnet die Möglichkeit, dass auch die Fachaufsichtsbehörde die notwendigen Festlegungen treffen kann. Dies dient insbesondere bei gleichartigen Abrufverfahren, die mehrere öffentliche Stellen anbieten wollen, der Vereinfachung.

10.9 Absatz 3 bestimmt, dass die Verantwortlichkeit für die Rechtmäßigkeit der Datenübermittlung im automatisierten Abrufverfahren auf Seiten des Empfängers der Daten liegt. Ein Abruf darf nur erfolgen, wenn die materiellen Voraussetzungen für eine Datenübermittlung vorliegen (zum Beispiel § 14 BbgDSG). Die Verlagerung der Verantwortlichkeit für die Übermittlung der Daten auf den Datenempfänger ist darin begründet, dass die übermittelnde Stelle im Einzelfall keinen Einfluss auf den Datenabruf hat. Die übermittelnde Stelle trägt jedoch insoweit Verantwortung, als sie anlassbezogen die Zulässigkeit der Datenübermittlung prüft, um bei eventuell festgestellten Verstößen die erforderlichen Maßnahmen ergreifen zu können, zum Beispiel die Beendigung des Abrufverfahrens, wenn sonst die schutzwürdigen Belange der Betroffenen verletzt sind oder die Anzeige einer Ordnungswidrigkeit beziehungsweise Straftat (§ 38 BbgDSG). Darüber hinaus ist die übermittelnde Stelle verpflichtet, durch geeignete technische und organisatorische Maßnahmen erfolgte Datenübermittlungen stichprobenartig zu überprüfen. Eine Überprüfung jeden Abrufs würde dem Sinn und Zweck der Einrichtung eines automatisierten Abrufverfahrens und der damit beabsichtigten Vereinfachung von Verwaltungsabläufen zuwiderlaufen. Die Größe der Stichprobe orientiert sich vor allem an der Sensibilität der abzurufenden Daten. Die diesbezüglichen Überlegungen sind Bestandteil des Sicherheitskonzepts nach § 7 Absatz 3 BbgDSG.

10.10 Sofern innerhalb einer öffentlichen Stelle automatisierte Verfahren zur Weitergabe von Daten im Sinne von § 14 Absatz 5 BbgDSG eingerichtet werden, gelten die vorstehenden Ausführungen entsprechend.

10.11 Die vorstehenden Ausführungen finden auf die Zulassung regelmäßiger Datenübermittlungen entsprechend Anwendung.

11 Zu § 10 Technische und organisatorische Maßnahmen

11.1 Datenverarbeitende Stellen oder die in ihrem Auftrag tätigen Stellen haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Brandenburgischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz zu gewährleisten. Die Verpflichtung zur Durchführung von Maßnahmen nach § 10 BbgDSG gilt für die automatisierte und nicht-automatisierte Datenverarbeitung, also auch für manuelle Karteien und Akten. Für den Bereich der Landesverwaltung ist die IT-Sicherheitsleitlinie der Landesregierung vom 22. September 2009 (ABl. S. 2090) zu beachten. Andere Stellen können diese Leitlinie zur Orientierung heranziehen oder diese für verbindlich erklären.

11.2 Die Überlegungen hinsichtlich der zu treffenden technischen und organisatorischen Maßnahmen sollten unmittelbar zu Beginn der Programmentwicklung angestellt werden. Nur so kann gewährleistet werden, dass die Anforderungen in die Ausschreibungen beziehungsweise in das Pflichtenheft aufgenommen und durch die Produkte später gewährleistet werden, ohne dass es kostenintensiver Nachrüstungen bedarf.

Es gilt dabei der Grundsatz der Verhältnismäßigkeit. Der Aufwand für die Maßnahmen hat in einem angemessenen Verhältnis zum angestrebten Schutzzweck zu stehen, wobei sich die Maßnahmen nach dem jeweiligen Stand der Technik richten. Stand der Technik sind am Markt verfügbare Produkte. Die Anforderungen an die zu treffenden Maßnahmen richten sich nach dem Schutzbedarf der personenbezogenen Daten. Je größer dieser ist, desto höhere Anforderungen sind an die zu treffenden technischen und organisatorischen Maßnahmen zu stellen.

11.3 Ob eine Maßnahme angemessen ist, kann nur anhand der konkreten Umstände des Einzelfalles entschieden werden. Dabei sind der vom Brandenburgischen Datenschutzgesetz oder von anderen datenschutzrechtlichen Vorschriften verlangte Schutz der Daten, das durch die Maßnahme erreichte Schutzniveau und der damit verbundene Aufwand zu betrachten. Ebenso ist das Ausmaß der zu erwartenden Schäden für die Rechte der Betroffenen in die Prüfung, ob eine Maßnahme beziehungsweise das hinsichtlich eines Verfahrens bestehende Schutzniveau angemessen ist, einzubeziehen.

11.4 Als Entscheidungshilfen bei der Angemessenheitsprüfung können neben der Art der verarbeiteten Daten und ihrer Schutzwürdigkeit auch die Menge der verarbeiteten Daten sowie die Art der eingesetzten Verfahren dienen. So erfordern zum Beispiel Angaben über gesundheitliche Verhältnisse, strafbare Handlungen, religiöse oder politische Anschauungen weitergehende Schutzvorkehrungen. Gleiches gilt, je mehr Daten über Betroffene gespeichert werden (zum Beispiel mit Hilfe einer Datenbank) oder bei der Verknüpfung mehrerer Datenbestände.

11.5 Es sind immer alle erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die Ausführung der Vorschriften des Brandenburgischen Datenschutzgesetzes zu gewährleisten. Soweit im Einzelfall eine Maßnahme nicht oder nicht vollständig umgesetzt wird, ist die dadurch entstehende Lücke durch entsprechende alternative Maßnahmen zur Erfüllung der Anforderungen zu schließen. Entscheidend ist das insgesamt gewährleistete Schutzniveau. Dieses bestimmt sich nach der Gesamtheit der getroffenen technischen und organisatorischen Maßnahmen. Die Datensicherheit ist dann ausreichend, wenn die getroffenen technischen und organisatorischen Maßnahmen in ihrer Gesamtheit einen hinreichenden Schutz gegen die Beeinträchtigung schutzwürdiger Interessen der Betroffenen beim Umgang mit ihren Daten gewährleisten.

11.6 Der zur Datensicherheit Verpflichtete muss in eigener Verantwortung unter den in Betracht kommenden technischen und organisatorischen Maßnahmen jene auswählen, die den vorgeschriebenen Schutz der Daten gewährleisten. Im Falle der Auftragsdatenverarbeitung wirken Auftraggeber und Auftragnehmer zusammen. Für das gesamte Verfahren trägt der Auftraggeber die Verantwortung.

11.7 § 7 Absatz 3 Satz 3 BbgDSG verpflichtet dazu, das Sicherheitskonzept fortzuschreiben, das heißt die Technikentwicklung zu beobachten und dementsprechend die Schutzmaßnahmen in angemessenen Abständen zu überprüfen und bei Bedarf nachzubessern.

11.8 Die in Absatz 2 neu eingeführten sechs Sicherheitsziele sind technologieunabhängig und zeigen einen Sicherheitsrahmen auf, der auch bei neuen Formen der Datenverarbeitung anwendbar ist. Das Brandenburgische Datenschutzgesetz greift teilweise die auch für die Sicherheit in der Informationstechnik (IT-Sicherheit) notwendigen Sicherheitsziele auf (Vertraulichkeit, Integrität, Verfügbarkeit), teilweise geht es mit den in Absatz 2 festgelegten weiteren Sicherheitszielen (Authentizität, Revisionsfähigkeit, Transparenz) im Interesse eines wirksamen Schutzes der personenbezogenen Daten darüber hinaus.

Gewährleistung der Sicherheitsziele:

a) Vertraulichkeit ist dann gewährleistet, wenn die gespeicherten Daten nicht in die Hände Unbefugter geraten können. Dieses Ziel kann durch verschiedene Maßnahmen erreicht werden. In Betracht kommen die Festlegung von Modalitäten zur Benutzeridentifikation und -autorisierung. Dies kann durch die Vergabe von Benutzername und Passwort, aber auch durch die Nutzung von Chipkarten und PIN erfolgen. Des Weiteren ist ein Berechtigungskonzept notwendig, damit Nutzer nur auf die tatsächlich benötigten Daten zugreifen können. Zu denken ist auch an die sichere Aufbewahrung oder Unterbringung der verwendeten Hardware und Backup-Datenträger, die Nutzung von Verschlüsselungssoftware bei der Speicherung in unsicheren Umgebungen (zum Beispiel Notebook, Laptop, lokaler PC) oder besonders sensibler Daten in Datenbanken und bei der Datenübertragung in Netzwerken oder die vertrauliche Behandlung von Angaben über verwendete Hard- und Software und die Systemkonfiguration.

b) Integrität ist gewährleistet, wenn die Datenbestände unversehrt, vollständig und aktuell sind, also verlässlich richtig. Integrität muss während aller Phasen der Datenverarbeitung von der Erhebung bis zur Sperrung/Löschung gegeben sein (vergleiche § 3 Absatz 2 BbgDSG). Unter anderem muss gewährleistet sein, dass Daten nicht durch Computerviren oder andere Schadsoftware verfälscht werden. Maßnahmen zur Sicherstellung der Integrität sind beispielsweise der Einsatz von digitalen Signaturen, Firewalls und Anti-Viren-Software, eine Plausibilitätskontrolle bei der Dateneingabe oder die Bildung und Kontrolle von Prüfsummen.

c) Verfügbarkeit bedeutet, dass die Daten zeitgerecht, das heißt in einer angemessenen Zeitdauer, zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können. Die Verfügbarkeit bezieht sich nicht nur auf die gespeicherten personenbezogenen Daten, sondern gleichermaßen auf die Hardware und die zur Verarbeitung erforderlichen Programme. Das Datenverarbeitungssystem ist hinsichtlich der Verfügbarkeit in seiner Gesamtheit zu betrachten. Welche Anforderungen hinsichtlich der Verfügbarkeit zu stellen sind, richtet sich vor allem nach der Art der Datenverarbeitungsprozesse. Im Sicherheitsbereich sind höhere Anforderungen zu stellen als beispielsweise bei Registraturverfahren. Verfügbarkeit kann gewährleistet werden durch Maßnahmen der Datensicherung, des Einsatzes redundanter Systeme (Ausweichrechenzentren, Server und Festplatten), unterbrechungsfreie Stromversorgung und der regelmäßigen Systemwartung.

d) Die Authentizität ist dann gewährleistet, wenn ein Dokument beziehungsweise Datum zweifelsfrei seinem Ursprung zugeordnet werden kann. Die Gewährleistung der Authentizität ist hauptsächlich bei elektronisch übertragenen Daten von Bedeutung. Den Gefährdungen kann durch Verfahren begegnet werden, bei denen die Herkunft der Daten nachvollziehbar ist. Bei der Bewertung der Verfahren sind verwendete Hardwarekomponenten und Programme einzubeziehen, zum Beispiel beim E-Government oder beim elektronischen Zahlungsverkehr. Beispiel: Einsatz von Signaturverfahren, bei denen rechtsverbindlich festgestellt werden kann, ob die Daten von den Betroffenen autorisiert (zum Beispiel digital signiert) sind oder wer Urheber von Daten ist, die nicht von den Betroffenen stammen (zum Beispiel bei Datenübermittlung).

e) Revisionsfähigkeit bedeutet, dass nachprüfbar ist, wie Daten in einen Datenbestand gelangt sind und welche Veränderungen sie im Laufe der Zeit durch

wen erfahren haben. Nachprüfbar muss sein, wer für das Aufnehmen bestimmter Daten in einen Datenbestand oder ihr Entfernen daraus die Verantwortung trägt. Dies kann durch entsprechende Protokolldateien gewährleistet werden, die jedoch selbst ein datenschutzrechtliches und personalrechtliches Risiko bergen und deshalb einer engen Zweckbindung nach § 29 Absatz 4 BbgDSG unterliegen.

f) Zur Herstellung von Transparenz sind automatisierte Verfahren in aktueller Form nachvollziehbar zu dokumentieren. Die einzelnen Verfahrensschritte müssen dabei so beschrieben werden, dass die Systematik der Prozesse ohne erheblichen zusätzlichen Aufwand nachvollziehbar wird. Transparenz wird vor allem durch die Dokumentation der Freigabe nach § 7 Absatz 3 BbgDSG und der gegebenenfalls durchzuführenden Vorabkontrolle nach § 10a BbgDSG, das ordnungsgemäße Führen des Verfahrensverzeichnisses sowie der Dokumentation von wesentlichen Programmänderungen beziehungsweise die laufende Fortschreibung der Programmdokumentation hergestellt.

11.9 Abhängig von den jeweiligen technischen Gegebenheiten sind im Einzelfall die Maßnahmen festzulegen, die den geforderten Sicherheitsrahmen erfüllen. Die Maßnahmen müssen zur Erreichung des angestrebten Schutzniveaus angemessen sein und das verbleibende Restrisiko tragbar machen. Dementsprechend ist vor dem Einsatz eines automatisierten Verfahrens gemäß § 7 Absatz 3 BbgDSG ein Sicherheitskonzept zu erstellen und dabei

a) der Grad der Schutzbedürftigkeit der personenbezogenen Daten festzustellen,

b) eine Bedrohungs- und Risikoanalyse durchzuführen,

c) geeignete und dem Stand der Technik entsprechende Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit zu bestimmen und umzusetzen sowie

d) eine entsprechende Kontrolle und Fortschreibung des Sicherheitskonzeptes zu gewährleisten.

11.10 Nicht-automatisierte Verfahren sind solche Verfahren, in denen die Verfahrensschritte ohne Hilfe programmgesteuerter Geräte ablaufen. Dabei ist es unerheblich, ob diesen Verfahren automatisierte Verfahren vorausgehen oder nachfolgen. Datenverarbeitung in nicht-automatisierten Verfahren findet zum Beispiel in manuellen Karteien, Sammlungen gleichartiger Formblätter oder herkömmlichen Akten statt.

11.11 Sammlungen von Datenträgern, die zugleich in automatisierten Verfahren verarbeitet werden, unterliegen hinsichtlich ihrer automatisierten Verarbeitung dem Absatz 2, hinsichtlich ihrer nicht-automatisierten Verarbeitung dem Absatz 3. Auch für diese Verfahren sind jedoch nach Absatz 1 geeignete technische und organisatorische Maßnahmen zu treffen, um der Beeinträchtigung schutzwürdiger Belange Betroffener entgegenzuwirken. Der Verhinderung des Zugriffs durch Unbefugte (Vertraulichkeit) kommt bei der nicht automatisierten Verarbeitung und bei Akten zentrale Bedeutung zu. Wenn dies erreicht ist, dann ist in aller Regel auch ausgeschlossen, dass jemand unbefugt Daten zur Kenntnis nehmen oder diese verändern oder löschen kann. Notwendigkeit und Umfang einzelner Maßnahmen der Datensicherheit beurteilen sich nach oben dargestellten Grundsätzen.

12 Zu § 10a Vorabkontrolle

12.1 Immer dann, wenn die Verarbeitung personenbezogener Daten besondere Risiken für die Rechte und Freiheiten der Betroffenen birgt, hat eine Vorabkontrolle dieser Datenverarbeitungen durch den behördlichen Datenschutzbeauftragten zu erfolgen. Die Vorabkontrolle ist, sofern sie erforderlich ist, Voraussetzung für die Freigabe der automatisierten Datenverarbeitung nach § 7 Absatz 3 BbgDSG.

12.2 Bei gemeinsamen Verfahren nach § 9 BbgDSG erfolgt die Vorabkontrolle durch den behördlichen Datenschutzbeauftragten der entsprechend der Vereinbarung nach § 9 Absatz 1a BbgDSG jeweils für die Freigabe verantwortlichen Stelle.

12.3 Sofern die zuständige oberste Landesbehörde oder die von ihr bestimmte Stelle gemäß § 7 Absatz 3 Satz 4 und 6 BbgDSG die Freigabe erklärt, kann eine gegebenenfalls im Vorfeld der Freigabe notwendige Vorabkontrolle durch den behördlichen Datenschutzbeauftragten der die Freigabe erklärenden Stelle erfolgen.

12.4 Absatz 2 bestimmt, in welchen Fällen besondere Risiken im Sinne von Absatz 1 Satz 1 insbesondere bestehen. Verfahren nach § 9 Absatz 1 BbgDSG bergen in aller Regel besondere Risiken für die Rechte der Betroffenen. Daher ist bei diesen Verfahren besonderes Augenmerk auf eine Vorabkontrolle zu legen, um die Rechte der Betroffenen angemessen zu schützen. Auch die Verarbeitung besonderer Arten von Daten sowie die Ausgabe mobiler personenbezogener Speicher- und Verarbeitungsmedien bergen besondere beziehungsweise spezifische Risiken für die Rechte und Freiheiten der Betroffen. Daher ist vor Beginn solcher Verarbeitungen immer eine Vorabkontrolle durchzuführen. Dies gilt auch für Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterfallen. Die Aufzählung in Absatz 2 ist nicht abschließend. Es sind darüber hinaus noch weitere Verfahren denkbar, bei denen eine Vorabkontrolle erforderlich ist. Hierbei kommt es auf eine Einzelfallbetrachtung an. Als Maßstab können beispielsweise die Menge der zu verarbeitenden personenbezogenen Daten, die betroffenen Personengruppen oder aber die Art der zu verarbeitenden Daten herangezogen werden. Aber auch weitere Gesichtspunkte, zum Beispiel eine beabsichtigte Verknüpfung verschiedener Datenbestände sind zu betrachten.

12.5 Gemäß Absatz 3 sind dem behördlichen Datenschutzbeauftragten insbesondere das Ergebnis der Risikoanalyse und das Sicherheitskonzept sowie die Angaben für das Verfahrensverzeichnis zuzuleiten. Es handelt sich hierbei um eine Bringschuld der Daten verarbeitenden Stelle gegenüber dem behördlichen Datenschutzbeauftragten. Die übergebenen Unterlagen müssen eine umfassende Prüfung des Verfahrens ermöglichen, so dass gegebenenfalls noch weitere als die vorgenannten Unterlagen zu übermitteln sind. Der behördliche Datenschutzbeauftragte führt die Vorabkontrolle auf der Grundlage der ihm übergebenen Unterlagen durch. Erst wenn das Ergebnis der Vorabkontrolle vorliegt, darf die Daten verarbeitende Stelle die Freigabe erklären (§ 7 Absatz 3 BbgDSG).

12.6 Im Rahmen der Vorabkontrolle wird durch den behördlichen Datenschutzbeauftragten insbesondere geprüft, ob das Verfahren datenschutzrechtlich zulässig ist, die Rechte der Betroffenen (vor allem auf Auskunft, Berichtigung und Löschung) gewahrt werden und die vorgesehenen technischen und organisatorischen Maßnahmen angesichts der besonderen Risiken des Verfahrens ausreichend sind.

12.7 In Zweifelsfällen hat der behördliche Datenschutzbeauftragte den LDA zu konsultieren. Dies bedeutet, dass dem LDA in diesem Fall die Gelegenheit gegeben werden muss, zu dem Verfahren eine Stellungnahme abzugeben. Hierfür ist eine angemessene Frist einzuplanen.

13 Zu § 11 Verarbeitung personenbezogener Daten im Auftrag

13.1 § 11 Absatz 1 BbgDSG ermächtigt Stellen des öffentlichen Bereiches personenbezogene Daten durch andere Stellen oder Personen im Rahmen eines Auftragsverhältnisses (Vertrages) verarbeiten zu lassen. Dabei bleibt der Auftraggeber für die Einhaltung des Datenschutzes verantwortlich und ist insofern auch die verantwortliche Stelle für den Fall, dass ein Betroffener seine Rechte geltend macht.

13.2 Unter Datenverarbeitung im Auftrag versteht man die Durchführung von Hilfs- beziehungsweise Unterstützungsarbeiten bei der Verarbeitung personenbezogener Daten durch eine andere Stelle in vollständiger Abhängigkeit und entsprechend den Weisungen des Auftraggebers. Die Weitergabe von Daten an den Auftragnehmer stellt keine Datenübermittlung an einen Dritten dar (siehe § 3 Absatz 2 Nummer 4 und Absatz 4 Nummer 3 BbgDSG und oben Nummern 3.8 sowie 3.16). Wird die Aufgabe der anderen Stelle demgegenüber zur selbständigen Erledigung übertragen, spricht man von einer Funktionsübertragung, die nicht unter § 11 BbgDSG fällt. Die Weitergabe der Daten an ein Unternehmen (private Stellen) oder eine andere öffentliche Stelle zur Durchführung der entsprechenden (Teil-) Aufgabe wäre eine Datenübermittlung, für die die Voraussetzungen des § 16 BbgDSG beziehungsweise § 14 BbgDSG vorliegen müssen.

13.3 Bevor ein Vertrag nach § 11 BbgDSG geschlossen wird, ist durch die Daten verarbeitende Stelle auch zu prüfen, wie eine ordnungsgemäße Datenverarbeitung sichergestellt werden kann, wenn der Vertrag endet, zum Beispiel nach einer fristlosen Kündigung wegen datenschutzrechtlicher Verstöße oder aber, wenn die Vertragspartner nach Vertragsende kein Interesse an der Verlängerung des Vertrages haben. In dem für das entsprechende Verfahren zu erstellende Sicherheitskonzept ist dieses Risiko zu betrachten und darzustellen, wie es beherrscht werden kann.

13.4 Gemäß § 11 Absatz 1 Satz 3 BbgDSG muss der Auftraggeber in den Fällen, in denen das Brandenburgische Datenschutzgesetz keine Anwendung auf den Auftragnehmer findet, vertraglich sicherstellen, dass die Vorschriften dieses Gesetzes befolgt und vom Auftraggeber veranlasste Kontrollen ermöglicht werden. Dies betrifft öffentliche Stellen als Auftragnehmer mit Sitz außerhalb des Landes Brandenburg sowie nicht-öffentliche Stellen. Veranlasste Kontrollen können auf dieser Grundlage beispielsweise vom behördlichen Datenschutzbeauftragten des Auftraggebers, von der örtlich zuständigen Kontrollbehörde oder bei nicht-öffentlichen Stellen im Land Brandenburg vom LDA Brandenburg vorgenommen werden.

13.5 Absatz 2 Satz 1 bestimmt Inhalt und Form des Vertrages. Die Schriftform ist sowohl für den Auftrag als auch für etwaige Unterauftragsverhältnisse sowie jede Ergänzung oder Änderung innerhalb des Auftragsverhältnisses zwingend. Darüber hinaus sind die in Absatz 2 genannten Mindestanforderungen für den Inhalt des Vertrages umzusetzen. Die entsprechenden Anforderungen sind detailliert zu regeln. Keinesfalls reicht eine Formulierung wie „die einschlägigen datenschutzrechtlichen Vorschriften sind zu beachten“ aus. Zu den erforderlichen Festlegungen des Auftraggebers gehören unter anderem die Abgrenzung der Verantwortungsbereiche von Auftraggeber und Auftragnehmer, Regelungen des Verfahrens zum Test und zur Freigabe der Programme, Verfahren zur Fortschreibung, Änderung, Löschung und Sperrung sowie die Vorgabe der erforderlichen technischen und organisatorischen Maßnahmen nach § 10 BbgDSG. Ist der Auftragnehmer eine nicht-öffentliche Stelle sollte vereinbart werden, dass nur Beschäftigte eingesetzt werden, die nach dem Verpflichtungsgesetz verpflichtet sind; dies kommt insbesondere in Betracht, wenn personenbezogene Daten verarbeitet werden, die durch Berufs- oder besondere Amtsgeheimnisse geschützt sind. Zu berücksichtigen ist, dass die Pflichten der Daten verarbeitenden Stelle insbesondere nach den §§ 7, 8, 10 und 10a BbgDSG fortbestehen und sich die entsprechenden Sicherheitskonzepte auch auf den Auftragnehmer beziehen müssen. Dieser kann die Daten verarbeitende Stelle bei der Erarbeitung der Unterlagen unterstützen. Sind im Vertrag Unterauftragsverhältnisse vorgesehen, so muss der Auftraggeber dafür sorgen, dass der Auftragnehmer mit dem Unterauftragnehmer Verträge abschließt, die die Einhaltung der gegenüber dem Auftraggeber bestehenden Pflichten gewährleisten, und

damit einen gleichwertigen Schutz der personenbezogenen Daten sicherstellt. Eine Checkliste, welche Regelungen in einem Vertrag nach § 11 BbgDSG mindestens zu vereinbaren sind, ist in Anlage 2 enthalten.

13.6 Nach Absatz 2 Satz 2 muss der Auftragnehmer die Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen nach § 10 BbgDSG bieten. Hiervon muss sich der Auftraggeber bei der Auswahl und im Rahmen der Durchführung des Auftragsverhältnisses überzeugen. Je nach Art des Auftrags kann hierfür ein Besuch vor Ort notwendig sein.

13.7 Besondere Maßnahmen bei der Auswahl und Beauftragung sind zu treffen, wenn die Daten einer gesetzlichen Geheimhaltungspflicht oder einem besonderen Berufs- oder Amtsgeheimnis unterliegen. Nicht-öffentliche Stellen sollen nur dann beauftragt werden, wenn keine schutzwürdigen Interessen des Betroffenen entgegenstehen.

13.8 Von der Möglichkeit der Auftragserteilung durch die Fachaufsichtsbehörde darf Gebrauch gemacht werden, wenn bei nachgeordneten Behörden mit gleicher Aufgabenstellung der Auftragnehmer aus Rationalisierungsgründen ein einheitliches Verfahren anwenden soll. Der Umfang der Weisungsbefugnisse von Fachaufsichtsbehörden und verantwortlicher Stelle gegenüber dem Auftragnehmer ist dabei eindeutig abzugrenzen.

13.9 Der Auftragnehmer darf Daten nur im Rahmen der Weisungen der Auftrag gebenden Stelle verarbeiten. Weisungen, die sich auf rechtswidrige Datenverarbeitungen beziehen, sind nicht auszuführen.

13.10 Vor einer Auftragserteilung an eine nicht-öffentliche Stelle ist zu prüfen, ob bereichsspezifische Regelungen zu beachten sind (zum Beispiel § 80 SGB X, § 35 des Brandenburgischen Meldegesetzes) oder die Verarbeitung personenbezogener Daten im Auftrag ausschließen (zum Beispiel im medizinischen Bereich wegen der ärztlichen Schweigepflicht).

13.11 Absatz 5 enthält eine Datenverarbeitungsbefugnis für die Fälle, in denen Dritte die Daten verarbeitende Stelle durch Gutachten oder sonstige eigenständige Leistungen unterstützen, also Tätigkeiten ausüben sollen, die teilweise weit über bloße Hilfs- beziehungsweise Unterstützungsarbeiten hinausgehen (siehe oben 13.2) und damit nicht mehr als Datenverarbeitung im Auftrag klassifiziert werden können. Dabei müssen den Experten oftmals personenbezogene Daten offen gelegt werden, zum Beispiel bei der anwaltlichen Beratung oder betriebswirtschaftlichen Untersuchungen. In diesen Fällen gelten die Vorschriften der Absätze 1 bis 3 entsprechend; darüber hinaus müssen die für eine Übermittlung der notwendigen Daten geltenden Anforderungen des Absatzes 5 vertraglich abgesichert werden. Die Auftrag gebende Stelle bleibt in diesen Fällen für die Einhaltung der datenschutzrechtlichen Anforderungen mit verantwortlich.

14 Zu § 11a Wartung

14.1 Datenverarbeitungssysteme müssen regelmäßig gewartet und gepflegt werden. Grundsätzlich wird die Wartung und Pflege von Soft- und Hardware von den Administratoren der jeweiligen öffentlichen Stellen beziehungsweise von privaten Dienstleistungsunternehmen vorgenommen.

14.2 Externe Personen oder Stellen, die mit der Wartung oder Systembetreuung von Einrichtungen zur automatisierten Datenverarbeitung betraut sind, haben nach den Weisungen des Auftraggebers zu arbeiten. Bezüglich der Vereinbarung nach Absatz 2 sind grundsätzlich die Regelungen zur Datenverarbeitung im Auftrag nach § 11 BbgDSG zu beachten. Hinsichtlich der Vertragsgestaltung sind die Anlagen 2 und 3 zu beachten.

14.3 Der Auftraggeber hat vor Beginn der Arbeiten durch technische und/oder organisatorische Maßnahmen sicherzustellen, dass der Auftragnehmer dabei möglichst keine personenbezogenen Daten einsehen kann beziehungsweise personenbezogene Daten nur zur Kenntnis genommen werden können, soweit dies unvermeidbar ist. Ziel ist es, den Zugriff auf personenbezogene Daten weitestgehend auszuschließen. Hiervon darf nur abgewichen werden, wenn die Kenntnisnahme personenbezogener Daten im konkreten Einzelfall unerlässlich ist. In diesem Fall sind die in Anlage 4 aufgeführten besonderen Anforderungen zu erfüllen und die Mitarbeiter von Wartungsfirmen gemäß §11a Absatz 2 Satz 3 BbgDSG vor der erstmaligen Ausführung von Arbeiten in besonderer Weise zu Verschwiegenheit zu verpflichten.

15 Zu § 12 Erhebung

15.1 Personenbezogene Daten dürfen nur erhoben werden, soweit ihre Kenntnis für die rechtmäßige Erfüllung der gesetzlich zugewiesenen Aufgabe erforderlich ist. Danach muss die erhebende Stelle für die Aufgabe, zu deren Erfüllung die Daten erhoben werden, zuständig sein und die zu erhebenden Daten müssen zur Erfüllung dieser Aufgabe erforderlich sein. Bei der Beurteilung der Erforderlichkeit ist ein strenger Maßstab anzulegen. Die Erhebung ist auf das zum Erreichen des angegebenen Zwecks erforderliche Minimum zu beschränken. Eine Erhebung personenbezogener Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken ist unzulässig.

15.2 Grundsätzlich sind personenbezogene Daten beim Betroffenen und mit dessen Kenntnis zu erheben. Er ist in jedem Fall über die für die Erhebung einschlägige Rechtsvorschrift aufzuklären, ferner über die Folgen der Verweigerung von Angaben (zum Beispiel Erfüllen eines Ordnungswidrigkeitentatbestandes, Ablehnung einer beantragten Leistung, eventuell verzögerte Bearbeitung wegen des Ausschlusses telefonischer Rückfragen bei Nichtangabe der Telefonnummer).

15.3 Ohne seine Kenntnis dürfen Daten beim Betroffenen nur unter sehr engen Voraussetzungen erhoben werden. Entweder muss eine Rechtsvorschrift dies vorsehen oder es ist zum Schutz von Leben und Gesundheit beziehungsweise zur Abwehr erheblicher Gefahren für die natürlichen Lebensgrundlagen erforderlich. Bei Dritten dürfen personenbezogene Daten ohne Kenntnis des Betroffenen nur unter den Voraussetzungen erhoben werden, nach denen eine nachträgliche Zweckänderung bereits erhobener Daten zulässig wäre (§ 13 Absatz 2 Satz 1 Buchstabe a und c bis f BbgDSG). Die Erhebung muss in jedem Fall verhältnismäßig sein. Das heißt, die Form der Erhebung muss geeignet sein und sie darf den Betroffenen nicht übermäßig in seinem Recht auf informationelle Selbstbestimmung einschränken. Von mehreren Möglichkeiten der Datenerhebung ist die Möglichkeit auszuwählen, die den Betroffenen in seinen Rechten am geringsten einschränkt und dennoch den Zweck erfüllt.

15.4 Die Hinweis- und Auskunftspflichten der Behörden gemäß Absatz 2 können gegebenenfalls zusammen mit den Hinweisen nach § 18 Absatz 2 BbgDSG zum Beispiel durch das Aushändigen von Merkblättern oder entsprechende Hinweise auf Antragsformularen und Bescheiden erfüllt werden.

16 Zu § 13 Zweckbindung bei Speicherung, Veränderung und Nutzung

16.1 Grundsätzlich dürfen personenbezogene Daten im Rahmen der rechtmäßigen Aufgabenerfüllung nur für die Zwecke gespeichert, verändert oder genutzt werden, für die sie erhoben wurden. Ein Zweck kann beispielsweise auch die Übermittlung der Daten an Dritte sein. Dies betrifft zum Beispiel das Melderegister, das Handelsregister oder das Grundbuch.

16.2 Als nicht erhoben gelten solche Daten, die der verantwortlichen Stelle ohne Anforderung zugegangen sind, zum Beispiel unverlangte Mitteilungen Dritter, im Rahmen einer Anzeige oder auf Grund besonderer Rechtsvorschrift durch öffentliche Stellen übermittelte Daten.

16.3 Bestehen in Fällen des Absatzes 1 Satz 2 Anhaltspunkte dafür, dass die personenbezogenen Daten der verantwortlichen Stelle unter Verletzung datenschutzrechtlicher Vorschriften zugegangen oder von ihr erhoben worden sind, dürfen diese nicht verarbeitet werden.

Die Pflicht zur Rechtmäßigkeit staatlichen Verwaltungshandelns verbietet es, bisher rechtswidrige Verfahrensweisen oder rechtswidrig zustande gekommene personenbezogene Datensammlungen durch den Beginn eines neuen Verwaltungsverfahrens mit dem Status der Rechtmäßigkeit zu versehen.

16.4 § 13 Absatz 2 BbgDSG enthält eine abschließende Aufzählung der Fälle, in denen vom Zweckbindungsgebot nach Absatz 1 abgewichen werden darf. Eine Pflicht zur Zweckänderung bei Vorliegen der Voraussetzungen besteht nicht. Bei jeder Fallgruppe ist das Gebot der Verhältnismäßigkeit zu beachten.

16.5 Unter den Begriff der Rechtsvorschrift nach § 13 Absatz 2 Buchstabe a BbgDSG fallen Gesetze, Rechtsverordnungen und Satzungen.

16.6 Hinsichtlich der Einwilligung des Betroffenen in eine zweckändernde Datenverarbeitung nach § 13 Absatz 2 Satz 1 Buchstabe b BbgDSG ist § 4 Absatz 1 und 2 BbgDSG zu beachten.

16.7 Buchstabe c, 1. Alternative stellt die Betroffenen von sie belastenden Mehrfacherhebungen frei. Buchstabe c, 2. Alternative erlaubt, soweit erforderlich, eine Zweckänderung zur Prüfung von Angaben der Betroffenen in anderen Verfahren. Dabei müssen tatsächliche Anhaltspunkte für die Unrichtigkeit der Angaben bestehen, zum Beispiel der begründete Verdacht der Leistungserschleichung. Nicht zulässig ist ein Abgleich zwischen verschiedenen Datenbeständen, um solche Verdachtsfälle zu ermitteln.

16.8 Wann eine Zweckänderung aus Gründen des Gemeinwohls im Sinne von § 13 Absatz 2 Buchstabe d BbgDSG erforderlich ist, muss unter Berücksichtigung der Rechtsprechung zum Gemeinwohl beziehungsweise zum Wohl der Allgemeinheit ermittelt werden. Der abstrakte Rechtsbegriff des Gemeinwohls deckt eine Vielzahl von Sachverhalten und Zwecken ab; er bedarf daher der Konkretisierung im einzelnen Fall (BVerfGE 24, 367, 403). Es ist von Fall zu Fall zu prüfen, ob übergeordnete Gründe vorliegen, die eine Beeinträchtigung von Einzelinteressen rechtfertigen. Dabei ist die Beachtung der Normen, die das Zusammenleben der Menschen verbindlich regeln und deren Beachtung im Ganzen als überragend notwendig angesehen werden muss, höher einzustufen als das Individualinteresse.

16.9 Es reicht aber nicht jeder Nachteil für das Gemeinwohl aus, die Zweckänderung zu rechtfertigen. Erforderlich ist die Abwehr eines erheblichen Nachteils. Hierzu ist eine Güterabwägung vorzunehmen, ob die Zweckänderung personenbezogener Daten zur Erreichung des Zwecks geeignet und erforderlich ist und bei einer Gesamtabwägung zwischen der Schwere des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe die Grenze des Zumutbaren noch gewahrt ist (BVerfGE 71, 183, 196; BVerfGE 78, 77, 85). Erhebliche Nachteile für das Gemeinwohl im Sinne von § 13 Absatz 2 Buchstabe d BbgDSG sind zum Beispiel gegeben, wenn sich die Voraussetzungen für eine Subvention nachträglich ändern oder gar entfallen.

16.10 Nicht jede Beeinträchtigung der Rechte einer anderen Person rechtfertigt eine Zweckänderung. Eine schwerwiegende Beeinträchtigung ist vor allem bei der Gefährdung bedeutsamer Rechtsgüter wie Leben, Gesundheit, Freiheit, nicht unwesentlicher Vermögenswerte sowie anderer strafrechtlich geschützter Güter anzunehmen. Es muss eine hinreichende Wahrscheinlichkeit geben, dass der Schaden in absehbarer Zeit eintritt, beziehungsweise der Schaden muss bereits entstanden sein. Bei der Güterabwägung der widerstreitenden Interessen muss das rechtliche Interesse privater Dritter das Interesse der

jeweils betroffenen Person am Ausschluss der Zweckänderung überwiegen. Ein rechtliches Interesse besteht, wenn Dritte personenbezogene Daten Betroffener zur Verfolgung von eigenen oder mandatierten Rechten benötigen.

16.11 Eine Zweckänderung gemäß § 13 Absatz 2 Buchstabe e BbgDSG ist nur zum Nutzen des Betroffenen zulässig und auch nur dann, wenn keine Zweifel daran bestehen, dass schutzwürdige Interessen nicht beeinträchtigt werden können.

16.12 Allgemein zugängliche Quellen sind insbesondere Veröffentlichungen in Zeitungen, im Rundfunk oder in Telefonbüchern und Adressbüchern sowie im Internet. Die entsprechenden Daten dürfen nur insoweit verarbeitet werden, als sie für die Aufgabenerfüllung tatsächlich erforderlich sind. Nur diesen Anforderungen genügende Daten kommen daher für eine Zweckänderung in Betracht. Schutzwürdige Interessen der Betroffenen an dem Ausschluss der Zweckänderung überwiegen offensichtlich, wenn es sich um lange zurückliegende Sachverhalte handelt und die zweckändernde Nutzung dem Betroffenen einen Nachteil zufügt, insbesondere wenn es sich beispielsweise um Daten über Vorstrafen handelt und ihre zeitlich unbeschränkte Verwendung die Resozialisierung gefährdet (Urteil des BVerfG vom 5. Juni 1973; BVerfGE 35, 202). Dies gilt im besonderen Maße, wenn ein Verwertungsverbot nach § 51 des Bundeszentralregistergesetzes besteht.

16.13 Eine Zweckänderung für Zwecke der Verfolgung von Straftaten oder Ordnungswidrigkeiten liegt nicht vor, wenn die öffentliche Stelle im Rahmen ihrer ureigenen Aufgabenstellung Ordnungswidrigkeiten verfolgt oder Straftaten zur Anzeige bringt. Adressaten dieser Regelung sind grundsätzlich diejenigen öffentlichen Stellen, die nicht originär mit Aufgaben der Strafverfolgung und der Ahndung von Ordnungswidrigkeiten betraut sind. Die Befugnisse der Polizei im Rahmen der Strafverfolgung und der Staatsanwaltschaft ergeben sich aus der Strafprozessordnung.

16.14 Die Befugnis für eine Zweckänderung nach Absatz 2 Satz 1 wird durch Satz 2 eingeschränkt. Danach ist eine Zweckänderung auf der Grundlage der Buchstaben c bis g unzulässig, wenn die Daten einem Berufs- oder besonderen Amtsgeheimnis unterliegen und der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind. Träger von Berufsgeheimnissen sind die in § 203 StGB genannten Berufsinhaber wie beispielsweise Ärzte, Rechtsanwälte, Wirtschafts- und Steuerberater oder Sozialarbeiter. Unter den Begriff des Amtsgeheimnisses fallen die durch besondere Rechtsvorschriften begründeten Geheimhaltungspflichten. Dazu zählen beispielsweise das Statistikgeheimnis, das Steuergeheimnis oder das Post- und Fernmeldegeheimnis. Eine zweckändernde Verarbeitung solcher Daten ist nur zulässig, wenn dies durch Rechtsvorschrift erlaubt ist oder der Betroffene eingewilligt hat.

16.15 Eine Zweckänderung nach Absatz 3 liegt dann nicht vor, wenn personenbezogene Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen verarbeitet oder genutzt werden. Die Organisationsuntersuchungen können auch von dienst- oder fachaufsichtsführenden Stellen durchgeführt werden. Im Rahmen der Ressortverantwortung ist es Sache der Ministerien, die Aufgabenerledigung im nachgeordneten Bereich zu steuern und zu beaufsichtigen. Sofern im Zusammenhang mit der Wahrnehmung von Aufsichts- oder Kontrollbefugnissen Verstöße aufgedeckt werden, ist die Verwendung der entsprechenden Daten zur dienst-, arbeits-, haftungs- oder strafrechtlichen Ahndung dieser Verstöße zulässig.

16.16 Eine Zweckänderung liegt auch dann nicht vor, wenn innerhalb der verantwortlichen Stelle personenbezogene Daten zu Ausbildungszwecken verarbeitet oder genutzt werden. Die Verwendung personenbezogener Daten muss jedoch für den beabsichtigten Zweck unerlässlich sein und überwiegende schutzwürdige Interessen der Betroffenen dürfen nicht entgegenstehen. Vorbehaltlich bereichsspezifischer Regelungen ist somit ausgeschlossen, dass Originalakten mit personenbezogenem Inhalt ohne Anonymisierung auch außerhalb der verantwortlichen Stelle zu Ausbildungszwecken verwendet werden.

17 Zu § 14 Übermittlung innerhalb des öffentlichen Bereichs

17.1 Absatz 1 erlaubt die Übermittlung personenbezogener Daten innerhalb des öffentlichen Bereichs materiell unter den gleichen Voraussetzungen, die auch für die Erhebung, Speicherung, Veränderung und Nutzung innerhalb der verantwortlichen Stelle gelten. Die Übermittlung muss im Rahmen des Erhebungszwecks liegen; anderenfalls müssen die Voraussetzungen für eine Zweckänderung im Sinne des § 13 Absatz 2 Satz 1 BbgDSG erfüllt sein. Auf die Ausführungen unter Nummer 16 wird insbesondere wegen des auch hier anzuwendenden Verhältnismäßigkeitsgrundsatzes verwiesen.

17.2 Als Datenempfänger kommen alle öffentlichen Stellen eines Landes oder des Bundes in Betracht.

17.3 Eine Übermittlung gehört zu den eigenen Aufgaben der verantwortlichen (übermittelnden) Stelle, wenn dieser Stelle Benachrichtigungs- oder Beteiligungspflichten obliegen (zum Beispiel Pflicht zur Beteiligung anderer Behörden im Rahmen der Erteilung einer Baugenehmigung). Gleiches gilt dann, wenn die Daten verarbeitende Stelle Daten ohne Ersuchen bei Vorliegen der Voraussetzungen des § 13 Absatz 2 Satz 1 Buchstabe d und g BbgDSG übermittelt.

17.4 Für die Erforderlichkeit einer Übermittlung nach § 14 Absatz 1 Satz 1, 2. Alternative BbgDSG, kommt es darauf an, ob der Dritte, an den die Daten übermittelt werden, auf die Kenntnis der Daten angewiesen ist. Nicht

entscheidend ist, ob er die Daten auch auf andere Weise erhalten kann. Bei einer Übermittlung auf Ersuchen kann grundsätzlich davon ausgegangen werden, dass seitens des Dritten geprüft worden ist, ob die Daten nicht vorrangig bei den Betroffenen zu erheben sind.

17.5 Bei der Übermittlung auf Ersuchen liegt grundsätzlich Amtshilfe vor. Das Übermittlungsersuchen ist, soweit nicht bereichsspezifische Regelungen wie beispielsweise §§ 111 bis 115 der Abgabenordnung oder §§ 3 bis 7 SGB X vorgehen, nach den §§ 4 bis 8 VwVfG zu behandeln. Sind die Voraussetzungen für eine Zweckänderung nach § 13 Absatz 2 BbgDSG nicht erfüllt, steht der Leistung von Amtshilfe ein rechtlicher Hinderungsgrund im Sinne des § 5 Absatz 2 Satz 1 Nummer 1 VwVfG entgegen. Hält sich die ersuchte Stelle nicht für verpflichtet, dem Übermittlungsersuchen nachzukommen, verfährt sie nach § 5 Absatz 5 VwVfG.

17.6 Das Übermittlungsersuchen muss so abgefasst sein, dass die ersuchte Stelle erkennen kann, ob die Übermittlung im Rahmen des Erhebungszwecks liegt oder die Voraussetzungen für eine Zweckänderung vorliegen. Für die Darlegung gilt der Grundsatz: Soviel Informationen wie nötig, so wenig Informationen wie möglich. Eine weitergehende Prüfung der Zulässigkeitsvoraussetzungen stellt die ersuchte Stelle nur dann an, wenn dazu besonderer Anlass besteht, zum Beispiel bei Zweifeln, ob der Dritte, an den die Daten übermittelt werden, die Daten erheben darf.

17.7 Fernmündliche Übermittlungen sind nur zulässig, soweit sich die mit der Übermittlung betraute Person von der Identität der Person, an die übermittelt wird, beispielsweise durch Rückruf überzeugt hat. Bei Übermittlungen per Telefax sollte auch geprüft werden, ob der Adressat unter der bekannten Anschlussnummer erreichbar ist.

17.8 Das Zweckbindungsgebot gilt auch für den Datenempfänger. Das heißt, er darf die Daten nur zu den Zwecken weiterverarbeiten, für die sie ihm übermittelt wurden. Eine Zweckänderung ist nur unter den Voraussetzungen des § 13 Absatz 2 BbgDSG zulässig.

17.9 Bei der Datenübermittlung ist auch § 4 Absatz 5 BbgDSG zu beachten. Das heißt, es ist darauf zu achten, dass eine Trennung der Daten nach den jeweiligen Zwecken und nach den unterschiedlichen Betroffenen möglich ist. Sind allerdings personenbezogene Daten in Akten derart verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, so ist die Übermittlung der Daten, die nicht für die jeweilige Aufgabe erforderlich sind, zulässig. Allerdings dürfen schutzwürdige Interessen des Betroffenen nicht entgegenstehen. In diesen Fällen muss eine Abwägung zwischen den Interessen der Verwaltung und den Rechten des Betroffenen stattfinden. Bei einer unverhältnismäßigen Beeinträchtigung der Rechte ist es gegebenenfalls notwendig, Aktenauszüge zu erstellen, die nur Daten des Betroffenen und diese auch nur für den jeweiligen Zweck enthalten. Denkbar ist die Übermittlung von Kopien, auf denen die betreffenden Daten geschwärzt wurden. Die Übermittlung von nicht benötigten Daten stellt einen absoluten Ausnahmefall dar. Sofern solche Daten übermittelt werden, dürfen diese vom Empfänger nicht verarbeitet oder sonst genutzt werden (Verwertungsverbot).

17.10 Die Vorschriften gelten uneingeschränkt auch für die Weitergabe von personenbezogenen Daten innerhalb einer Behörde, zum Beispiel wenn Daten zwischen zwei Ämtern einer Behörde weitergegeben werden sollen oder aber für die Datenweitergabe von der Kommunalverwaltung zur Gemeindevertretung. Für einzelne Bereiche gibt es Spezialvorschriften, die den Regelungen des Brandenburgischen Datenschutzgesetzes vorgehen, beispielsweise im Bereich des Meldewesens (§ 28 Absatz 4 BbgMeldeG).

17.11 Die Vorlage von Verwaltungsvorgängen und die Erteilung von Auskünften in verwaltungsgerichtlichen Verfahren werden durch § 14 BbgDSG nicht berührt. Sie richten sich nach § 99 der Verwaltungsgerichtsordnung.

18 Zu § 15 Übermittlung an öffentlich-rechtliche Religionsgemeinschaften

18.1 Kirchen, Religionsgesellschaften und Weltanschauungsgemeinschaften des öffentlichen Rechts werden bei der Übermittlung wie Stellen innerhalb des öffentlichen Bereichs behandelt. An sie können unter den gleichen Voraussetzungen wie an öffentliche Stellen personenbezogene Daten übermittelt werden; sie müssen aber ausreichende Datenschutzmaßnahmen getroffen haben. Diese Anforderung ist bei den anerkannten öffentlich-rechtlichen Religionsgemeinschaften ohne weitere Prüfung durch die verantwortliche Stelle als erfüllt anzusehen.

18.2 Nicht zu den öffentlich-rechtlichen Religionsgemeinschaften gehören die privatrechtlich organisierten Einrichtungen und Werke der Kirchen (zum Beispiel Diakonisches Werk, Caritas). Übermittlungen an diese Stellen sind nach den Vorschriften für die Übermittlung an Personen und Stellen außerhalb des öffentlichen Bereichs zu beurteilen.

19 Zu § 16 Übermittlung an Personen und Stellen außerhalb des öffentlichen Bereichs

19.1 § 16 BbgDSG begründet keinen Anspruch privater Dritter auf Übermittlung personenbezogener Daten. Wenn sich ein solcher Anspruch nicht aus anderen Rechtsvorschriften ergibt, steht die Übermittlung bei Vorliegen der übrigen Voraussetzungen im pflichtgemäßen Ermessen der verantwortlichen Stelle.

19.2 Die Stellen nach § 2 Absatz 2 Satz 1 BbgDSG, also die Eigenbetriebe, öffentlichen Stellen, die nach der Eigenbetriebsverordnung geführt werden, und die der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen, werden, soweit sie die Daten für die Verfolgung wirt-

schaftlicher Zwecke benötigen, den privaten Stellen gleichgestellt.

19.3 Sofern die Datenübermittlung unter den Voraussetzungen des § 16 Absatz 1 Buchstabe a und b BbgDSG erfolgt, wird auf die Ausführungen unter Nummer 16 sowie 17.3 verwiesen.

19.4 Ein rechtliches Interesse im Sinne von Buchstabe c besteht zum Beispiel dann, wenn die Daten zur Geltendmachung von Rechtsansprüchen, beispielsweise zur Adressermittlung im Zusammenhang mit Schadensersatzforderungen oder zur Schuldnerermittlung benötigt werden. Das Interesse muss glaubhaft gemacht werden. Das heißt, die Tatsachen, die ein rechtliches Interesse begründen, müssen plausibel dargelegt werden. Sie müssen jedoch nicht bewiesen werden. Weiterhin muss eine Interessenabwägung zwischen dem rechtlichen Interesse am Erhalt der Daten und dem Geheimhaltungsinteresse des Betroffenen stattfinden. Dabei müssen der Behörde gegebenenfalls Anhaltspunkte für ein Geheimhaltungsinteresse vorliegen. Nachforschungen müssen diesbezüglich nicht angestellt werden. Zu beachten ist, dass möglicherweise bereichsspezifische Rechtsvorschriften einer Übermittlung entgegenstehen. In diesen Fällen muss die Übermittlung trotz Vorliegen eines rechtlichen Interesses unterbleiben.

19.5 Ein berechtigtes Interesse im Sinne von Buchstabe d kann auch ein wirtschaftliches Interesse sein. Dieses Interesse ist geringer einzustufen als das rechtliche Interesse im Sinne von Buchstabe c. Die Übermittlung ist zulässig, wenn ihr der Betroffene nach einer entsprechenden Information gemäß Absatz 2 nicht widersprochen hat. Die Information bezüglich einer beabsichtigten Übermittlung kann bereits bei der Erhebung erfolgen (zum Beispiel mit dem bei der Erhebung verwendeten Vordruck). Auch der Widerspruch kann bereits bei der Erhebung geltend gemacht werden. Bei einer Vielzahl von beabsichtigten Übermittlungen können die Betroffenen auch allgemein zum Beispiel über die Presse oder durch Postwurfsendungen informiert werden.

20 Zu § 17 Übermittlung an ausländische und internationale Stellen

20.1 Für den Datentransfer in Mitgliedstaaten der Europäischen Union (EU) und die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum sowie an Organe und Einrichtungen der Europäischen Gemeinschaften gelten die gleichen Vorschriften wie für den Datenverkehr im Inland. Das heißt, die Zulässigkeit richtet sich nach § 4 BbgDSG.

20.2 Für Datenübermittlungen an Stellen außerhalb der EU sowie an über- und zwischenstaatliche Stellen gelten die gleichen Zulässigkeitsvoraussetzungen wie für die Datenübermittlungen an Stellen außerhalb des öffentlichen Bereichs mit der Maßgabe, dass sie darüber hinaus nur zulässig sind, wenn dort ein angemessenes Datenschutzniveau vorliegt. Um das Datenschutzniveau zu beurteilen, sind insbesondere die rechtlichen Rahmenbedingungen beim Datenempfänger für die beabsichtigte Übermittlung heranzuziehen. Im Übrigen wird das Datenschutzniveau von Drittländern durch die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie beurteilt und eine Stellungnahme hierzu abgegeben. Mit dem 1. Juli 2000 ist die EU-Datenschutzrichtlinie von den Staaten des Europäischen Wirtschaftsraumes (EWR-Staaten, dies sind die EU-Staaten sowie Norwegen, Island und Liechtenstein) übernommen worden. Danach gilt das Gebot des freien Datenverkehrs zwischen EU-Staaten und den übrigen EWR-Staaten. Somit ist davon auszugehen, dass in allen EWR-Staaten ein ausreichendes Datenschutzniveau besteht. Informationen darüber, in welchen weiteren Ländern die Datenschutzgruppe eine Stellungnahme bezüglich des Datenschutzniveaus abgegeben hat, können beim Ministerium des Innern des Landes Brandenburg eingeholt oder auf der entsprechenden Internetseite der EU unter folgendem Link abgerufen werden: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm.

20.3 Eine Datenübermittlung an Stellen ohne angemessenes Datenschutzniveau greift in hohem Maße in die Rechte der Betroffenen ein. Deshalb ist sie nur in den in Absatz 4 abschließend genannten Fällen zulässig. Hierzu gehört die Wahrung überwiegender öffentlicher Interessen im Sinne von Nummer 4. Vergleiche hierzu auch § 16 Absatz 1 Buchstabe d BbgDSG, der als Zulässigkeitsvoraussetzung lediglich das Vorliegen eines öffentlichen Interesses, und nicht wie hier eines wichtigen öffentlichen Interesses, vorschreibt. Der Begriff „lebenswichtige Interessen“ im Sinne von Nummer 5 stellt auf Rechtsgüter wie Leib, Leben und Gesundheit ab. Eine Übermittlung ist auch dann zulässig, wenn der Datenempfänger ausreichende Garantien zum Schutz der Persönlichkeitsrechte vorweist. Dies kann zum Beispiel durch Verträge zwischen Übermittler und Empfänger geschehen.

20.4 Sofern eine Übermittlung an Empfänger außerhalb der EU erfolgt, die kein angemessenes Datenschutzniveau aufweisen, ist dies dem Ministerium des Innern mitzuteilen.

20.5 Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Dies gilt vorbehaltlich besonderer Rechtsvorschriften auch für Übermittlungen auf Grund supranationalen Rechts oder eines ratifizierten Staatsvertrages.

21 Zu § 18 Auskunft und Einsicht in Akten

21.1 Der Auskunftsanspruch gehört neben den Ansprüchen auf Berichtigung, Löschung und Sperrung (§ 19 BbgDSG) zu den grundlegenden Rechten des Betroffenen. Er besteht unabhängig von dem Recht auf Akteneinsicht nach dem Akteneinsichts- und Informationszugangsgesetz (AIG). Der Auskunftsanspruch nach § 18 BbgDSG kommt nur dann nicht zum Zuge, wenn in anderen, spezielleren Gesetzen ein solcher Anspruch des Betroffe-

nen auf Auskunft über die zu seiner Person gespeicherten Daten besteht (zum Beispiel Brandenburgisches Polizeigesetz, Brandenburgisches Verfassungsschutzgesetz).

21.2 In laufenden Verwaltungsverfahren (§ 9 VwVfG in Verbindung mit § 1 Absatz 1 VwVfGBbg) haben die Vorschriften des Verwaltungsverfahrensgesetzes Vorrang vor den Vorschriften des Datenschutzgesetzes; vergleiche hierzu Nummer 2.11. Das heißt, dass während eines laufenden Verwaltungsverfahrens die Ansprüche von Verfahrensbeteiligten (siehe § 13 VwVfG in Verbindung mit § 1 Absatz 1 VwVfGBbg) auf Akteneinsicht nach § 29 VwVfG in Verbindung mit § 1 Absatz 1 VwVfGBbg zu beurteilen sind.

21.3 Auf der Grundlage des § 18 BbgDSG kann ein Bürger ohne Nennung eines besonderen Grundes gegenüber jeder öffentlichen Stelle seinen Anspruch auf Auskunft über die zu seiner Person gespeicherten und anderweitig verarbeiteten Daten geltend machen. Der Anspruch umfasst grundsätzlich sowohl alle zur Person des Betroffenen gespeicherten Daten, auch solche in Akten, als auch zu welchem Zweck und auf welcher Rechtsgrundlage seine Daten verarbeitet werden. Er bezieht sich darüber hinaus auf die Herkunft der Daten und die Empfänger übermittelter Daten, soweit diese bei der Daten verarbeitenden Stelle gespeichert sind. Des Weiteren sind die Empfänger von regelmäßigen Übermittlungen anzugeben. In der Auskunft müssen auch die Teilnehmer eines automatisierten Abrufverfahrens genannt werden, selbst wenn bisher keine Übermittlung stattgefunden hat.

21.4 Absatz 1 Satz 2 bestimmt, dass die Auskunft nicht erteilt wird, wenn personenbezogene Daten nur auf Grund gesetzlicher Aufbewahrungspflichten gespeichert sind und deshalb nicht gelöscht werden dürfen. Das Gleiche trifft zu, wenn die Daten ausschließlich zu Zwecken der Datensicherung oder Datenschutzkontrolle gespeichert wurden (zum Beispiel Datensicherungsbänder zur möglichen Rekonstruktion von aktuellen Datenbeständen).

21.5 Die Daten verarbeitende Stelle bestimmt das Verfahren und insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen. Sind die Daten in Akten gespeichert, kann dem Betroffenen auf Verlangen auch Einsicht gewährt werden. Diese Akteneinsicht ist jedoch nur auf die Teile der Akte beschränkt, die personenbezogene Daten des Betroffenen enthält. Eine darüber hinausgehende Akteneinsicht wäre unter Umständen auf der Grundlage des Verwaltungsverfahrensgesetzes für das Land Brandenburg oder nach dem Akteneinsichts- und Informationszugangsgesetz möglich. Hinsichtlich der weiteren Möglichkeiten für die Akteneinsicht besteht gemäß § 25 VwVfG in Verbindung mit § 1 Absatz 1 VwVfGBbg eine Beratungs- beziehungsweise Unterrichtungspflicht der öffentlichen Stelle gegenüber dem Betroffenen. Die Gewährung der Auskunft aus Akten oder Akteneinsicht wird unter dem Vorbehalt gewährt, dass der Betroffene Angaben macht, die das Auffinden und Auswerten der Daten mit einem angemessenen Aufwand ermöglicht.

21.6 Für die Auskunftserteilung und Akteneinsicht werden keine Gebühren erhoben. Die Erstattung eventueller Auslagen, wie zum Beispiel für die Anfertigung von Kopien, kann verlangt werden. Es ist zulässig, sich bei der Akteneinsicht Notizen zu machen oder Kopien anfertigen zu lassen. Bei der Auskunft aus automatisierter Verarbeitung kann ein Ausdruck des entsprechenden Datensatzes erfolgen.

21.7 Zuständig für die Auskunftserteilung ist die Daten verarbeitende Stelle. Gehen Auskunftsersuchen bei Auftragnehmern nach § 11 BbgDSG ein, sind diese an den Auftraggeber weiterzuleiten, sofern nicht der Auftragnehmer zur Auskunftserteilung berechtigt worden ist. Bei der Auskunftserteilung muss die Identität von Antragstellern hinreichend überprüft sein. Fernmündliche Auskünfte sind nur zulässig, wenn die Antrag stellende Person eindeutig identifiziert werden kann (zum Beispiel durch Rückruf).

21.8 Die Auskunftspflicht entfällt, wenn personenbezogene Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift geheim gehalten werden müssen oder eine Einzelabwägung ergibt, dass wegen der überwiegenden berechtigten Interessen eines Dritten (§ 3 Absatz 4 Nummer 3 BbgDSG) das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

21.9 Die Daten verarbeitende Stelle hat jede Ablehnung einer Auskunftserteilung zu begründen. Nur wenn hierdurch der Zweck der Auskunftsverweigerung gefährdet würde, darf eine Begründung unterbleiben.

21.10 Anträgen auf Auskunftserteilung und Akteneinsicht im Hinblick auf die Herkunft der Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft, der Polizei, unter bestimmten Voraussetzungen der Landesfinanzbehörden sowie von den in § 19 Absatz 3 BDSG genannten Bundesbehörden darf nur mit deren Zustimmung stattgegeben werden. Dies gilt ebenso für die Übermittlung personenbezogener Daten an diese Behörden. Für Landesbehörden gelten bei der Versagung der Zustimmung die Absätze 3 und 4 entsprechend.

21.11 Wird dem Betroffenen keine Auskunft erteilt, so richtet sich auf sein Verlangen hin das weitere Verfahren nach Absatz 6. Der LDA kann dann prüfen, ob die Auskunftsverweigerung rechtmäßig ist. Nur in besonders begründeten Einzelfällen darf auch dem LDA keine Auskunft erteilt werden. Diese Entscheidung trifft die zuständige oberste Landesbehörde.

22 Zu § 31 Verarbeitung personenbezogener Daten durch den Landtag

22.1 Die Vorschrift in Absatz 1 dient als Befugnisnorm der ausdrücklichen Klarstellung der Rechtslage für die Landesregierung zur Übermittlung personenbezogener Daten an den Landtag im Rahmen seiner parlamentarischen Aufgaben. Zu den parlamentarischen Aufgaben des Landtages auch im datenschutzrechtlichen Sinne ge-

hören unter anderem die Bearbeitung von Petitionen, die Aufbewahrung und Archivierung von parlamentarischen Unterlagen sowie die Einrichtung und Nutzung eines Dokumentations- und Informationssystems. Auch die Regierungskontrolle in Form von Kleinen und Großen sowie Mündlichen Anfragen und die Arbeit von Untersuchungsausschüssen zählen zu diesem Aufgabenkreis.

22.2 Oft ist die Landesregierung bei der Durchführung und Erfüllung dieser Aufgaben gehalten, personenbezogene Daten zu übermitteln. In diesen Fällen stellt sich regelmäßig die Frage nach der Zulässigkeit dieser Übermittlungen, weil sich hier das verfassungsmäßige Recht auf informationelle Selbstbestimmung (Artikel 11 der Landesverfassung) und das verfassungsmäßige Recht der Abgeordneten auf Information (Artikel 56 der Landesverfassung) überschneiden. Beide Rechte sind einander so zuzuordnen, dass sie soweit wie möglich ihre Wirkung entfalten können. Eine Auskunftserteilung darf nur ausnahmsweise verweigert werden, wenn besonders sensible Daten betroffen sind.

22.3 Die Landesregierung hat in jedem Fall zu prüfen, ob der Übermittlung der Daten an den Landtag überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Wenn dies bejaht wird, darf eine Übermittlung insoweit an den Landtag nicht erfolgen. Das Vorliegen solcher überwiegender schutzwürdiger Interessen ist nicht pauschal zu bestimmen, sondern bedarf einer genauen Prüfung jedes Einzelfalles. Die Rechtsprechung geht davon aus, dass sich die Schutzwürdigkeit individueller Belange ohne Berücksichtigung der beabsichtigten Verwendung der jeweiligen personenbezogenen Daten nicht konkretisieren lässt. In jedem Fall wird jedoch bei Daten der in § 4a BbgDSG genannten Kategorien eine besondere Schutzbedürftigkeit vorauszusetzen sein, die im Fall einer beabsichtigten Übermittlung eine Einzelfallprüfung erforderlich machen.

22.4 Unbeschadet der Datenschutzordnung des Landtages wird durch Absatz 2 vorgegeben, in welchem Umfang die von der Landesregierung übermittelten personenbezogenen Daten durch den Landtag veröffentlicht werden dürfen. Bei der Beantwortung parlamentarischer Anfragen ist regelmäßig davon auszugehen, dass die Antworten in Landtagsdrucksachen aufgenommen werden. Deswegen ist in diesem Zusammenhang eine Übermittlung personenbezogener Daten regelmäßig unzulässig, es sei denn, es bestehen keine Anhaltspunkte, dass schutzwürdige Belange der Betroffenen beeinträchtigt werden. Sofern für die Tätigkeit des Landtags erforderlich, können diese Angaben jedoch mündlich durch die Landesregierung in nicht-öffentlicher Sitzung erteilt oder Abgeordneten in persönlich adressierten Schreiben mitgeteilt werden, sofern nicht aufgrund besonderer Umstände auch hier die schutzwürdigen Interessen des Betroffenen an der Geheimhaltung seiner Daten das Informationsinteresse der Abgeordneten überwiegen.

23 Zu § 33c Videobeobachtung und -aufzeichnung

23.1 In Absatz 1 werden die Zwecke, zu denen eine Videoüberwachung erfolgen darf, genannt. Erfasst sind sowohl die reine Videobeobachtung als auch die Videoaufzeichnung. Bei der Videobeobachtung wird ein durch eine Kamera aufgenommenes Bild nur auf einen Bildschirm übertragen, ohne dass eine Aufzeichnung erfolgt. Bei der Videoaufzeichnung wird das gewonnene Bildmaterial aufgezeichnet, das heißt gespeichert. Beide Verfahren sind nur zulässig, wenn dies für die in Absatz 1 genannten Zwecke erforderlich ist und überwiegende schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden.

23.2 Der Begriff des „öffentlich zugänglichen Raumes“ ist weder in Rechtsprechung noch in der Literatur definiert. Das entscheidende Kriterium dabei ist nicht die Existenz eines Raumes im engeren Sinne, sondern die Zugänglichkeit des betreffenden Bereiches für die Öffentlichkeit beziehungsweise Allgemeinheit in enger Verknüpfung mit der jeweiligen sachlichen oder örtlichen Zuständigkeit einer öffentlichen Stelle für diesen Bereich. Dazu können beispielsweise der Eingangsbereich vor dem Gebäude einer Behörde, Räume innerhalb eines Dienstgebäudes aber auch der Parkplatz einer öffentlichen Stelle gehören, soweit er für den Publikumsverkehr geöffnet ist. Hiervon abzugrenzen ist das öffentliche Straßenland, wozu öffentlich zugängliche Gehwege, Straßen und Plätze gehören. Eine Videoüberwachung dieser Bereiche kann nicht auf § 33c BbgDSG gestützt werden (siehe Nummer 23.7).

23.3 Der Umstand der Videoüberwachung sowie die verantwortliche Stelle sind durch geeignete Maßnahmen kenntlich zu machen. Hierzu kann beispielsweise das Kennzeichen nach DIN 33450 verwendet werden.

23.4 Für die Videoüberwachung gelten im Übrigen die allgemeinen Regelungen des Brandenburgischen Datenschutzgesetzes. Das heißt zum Beispiel, dass vor dem Einsatz des Verfahrens ein Freigabeverfahren gemäß § 7 Absatz 3 BbgDSG und gegebenenfalls eine Vorabkontrolle gemäß § 10a BbgDSG durchzuführen ist. Sofern eine Videoaufzeichnung erfolgt, ist im Rahmen des Freigabeverfahrens auch zu untersuchen, innerhalb welcher Zeit die aufgezeichneten Daten zu löschen sind. Hierbei sind insbesondere die Regelungen des § 7 Absatz 1 Satz 2 und des § 19 Absatz 2 BbgDSG zu berücksichtigen. Es ist ein Verfahrensverzeichnis nach § 8 BbgDSG zu erstellen.

23.5 Die Verarbeitung zu anderen Zwecken (§ 33c Absatz 3 Satz 2 BbgDSG) ist begrenzt auf die Fälle, in denen eine Verarbeitung zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist. Das heißt, ein genereller Rückgriff auf § 13 Absatz 2 BbgDSG ist nicht zulässig. Daneben ist eine Zweckänderung jedoch mit Einwilligung des Betroffenen oder auf der Grundlage vorgehender spezieller Rechtsvorschriften möglich.

23.6 Nach Absatz 4 ist der Betroffene auf eine Veränderung, Übermittlung oder sonstige Nutzung der durch Videoaufnahmen gewonnenen Daten hinzuweisen. Die Benachrichtigung hat spätestens dann zu erfolgen, wenn der mit der Veränderung, Übermittlung, oder sonstigen Nutzung verfolgte Zweck nicht mehr gefährdet ist. Hierunter fallen zum Beispiel Maßnahmen der Strafverfolgung.

23.7 Spezielle Rechtsvorschriften über den Einsatz von Videokameras gehen gemäß § 1 Absatz 3 BbgDSG den Vorschriften der allgemeinen Regelungen des Brandenburgischen Datenschutzgesetzes vor (zum Beispiel § 31 BbgPolG oder § 6 BbgVerfSchG). Ebenso bietet § 33c BbgDSG keine Rechtsgrundlage für die Videoüberwachung des öffentlichen Straßenlandes oder nicht öffentlich zugänglicher Räume.

24 Zu § 38 Ordnungswidrigkeiten, Strafvorschrift

24.1 Verstöße gegen datenschutzrechtliche Vorschriften stellen einen Ordnungswidrigkeitentatbestand dar. Dabei ist gemäß § 10 des Ordnungswidrigkeitengesetzes (OWiG) nur vorsätzliches Handeln zu ahnden. Vorsätzliches Verletzen von datenschutzrechtlichen Vorschriften mit Sanktionen zu belegen, liegt dabei grundsätzlich im öffentlichen Interesse. Die Verfolgung von Ordnungswidrigkeiten liegt jedoch im Ermessen der zuständigen Ordnungsbehörde (Opportunitätsprinzip).

24.2 Die Strafnormen des Gesetzes finden nur dann Anwendung, wenn die Tat nicht nach anderen Vorschriften, insbesondere des Bundesrechts, strafbar ist.

24.3 § 38 BbgDSG ist eine sogenannte Blankettnorm, das heißt, ob ein Handeln oder Dulden strafbewehrt ist oder nicht, ergibt sich erst aus der Anwendung anderer Normen. Die Strafbestimmungen des Brandenburgischen Datenschutzgesetzes gelten auf Grund seiner Eigenschaft als Querschnittsgesetz sowohl bei der Verletzung der Bestimmungen des Brandenburgischen Datenschutzgesetzes selbst als auch für die Ahndung rechtswidriger Handlungen gegen nicht gesondert strafbewehrte bereichsspezifische Datenschutzvorschriften.

24.4 Für die Durchführung von Ordnungswidrigkeitenverfahren nach § 38 BbgDSG ist entsprechend der Vorschrift des § 36 Absatz 1 Nummer 1 OWiG in Verbindung mit § 23 Abs 8 BbgDSG der LDA zuständig.

24.5 Gemäß Absatz 3 ist ein Fehlverhalten dann mit Geld- oder Freiheitsstrafe bewehrt, wenn der Täter in Bereicherungs- oder Schädigungsabsicht handelt.

24.6 Eine Straftat nach § 38 BbgDSG wird nur auf Antrag verfolgt. Antragsbefugt sind der Betroffene, die verantwortliche Stelle und der LDA.

25 Inkrafttreten

Die Verwaltungsvorschrift tritt am Tag nach ihrer Veröffentlichung in Kraft.

VV-BbgDSG
Anlage 1 zu Nummer 9.1

Hinweise des Ministeriums des Innern vom 14. Oktober 2009 zur Verordnung zum Verfahrensverzeichnis (VerfVerzV) vom 10. September 2009 (GVBl. II S. 649)

In der oben genannten Verordnung hat die Landesregierung auf der Grundlage von § 8 Absatz 6 BbgDSG Regelungen bezüglich der Erstellung von Verzeichnissen über die bei der automatisierten Verarbeitung personenbezogener Daten angewendeten Verfahren getroffen. Nachfolgend werden diese Regelungen erläutert und Hinweise zum Ausfüllen des Musterformblattes für das Verfahrensverzeichnis gegeben. Hierbei werden nur die Punkte erläutert, die nicht selbsterklärend sind.

1 Erläuterung der Verordnung zum Verfahrensverzeichnis

§ 1 Absatz 1 VerfVerzV entspricht sinngemäß dem § 1 Absatz 1 der Verordnung zum Verfahrens- und Anlagenverzeichnis vom 23. November 1999 (GVBl. II S. 646). Das Musterformblatt zum Verfahrensverzeichnis wurde an die Änderungen der §§ 8 und 10 BbgDSG angepasst. Hinweise zum Ausfüllen des Musterformblattes werden unter Nummer 2 gegeben.

Zweck des Verfahrensverzeichnisses ist es, in komprimierter Form eine Übersicht über die einem konkreten Verfahren zugrundeliegenden, aus datenschutzrechtlicher Sicht wesentlichen Gesichtspunkte zu erhalten. Diese Übersicht dient zum einen der Selbstkontrolle der Daten verarbeitenden Stelle und zum anderen im Wege der Einsichtnahme in das Verzeichnis konkreter Verfahren der Transparenz der Datenverarbeitung für Betroffene.

Wie bisher ist das Verfahrensverzeichnis unverzüglich nach Beginn der jeweiligen automatisierten Verarbeitung personenbezogener Daten zu erstellen. Die hierfür im Wesentlichen erforderlichen Angaben sind aus dem Sicherheitskonzept nach § 7 Absatz 3 BbgDSG zu entnehmen.

§ 1 Absatz 2 enthält Regelungen für den Fall, dass mehrere öffentliche Stellen Verfahren zur automatisierten Verarbeitung personenbezogener Daten gemeinsam und/oder zentral betreiben oder betreiben lassen. Die für den zentralen Betrieb verantwortliche Stelle hat für die zentral betriebenen Komponenten oder Teilverfahren das Verfahrensverzeichnis zu fertigen und den das Verfahren nutzenden Stellen zur Verfügung zu stellen. Eine entsprechende Verpflichtung enthält § 2 Satz 2. Dies wird vor allem die Angaben zu den Nummern 9 und 11 (bezogen auf zentral bereit gestellte beziehungsweise genutzte Komponenten) betreffen. Die das Verfahren nutzenden Stellen haben, entsprechend ihrer Verantwortung für die materielle Rechtmäßigkeit des Verfahrens sowie für die Maßnahme nach § 10 BbgDSG, für ihren Bereich die Angaben für das Verfahrensverzeichnis festzulegen. Dies wird in der Regel die verbleibenden Punkte sowie die auf die dezentralen Komponenten bezogenen Angaben zu den Nummern 9 und 11 des Verfahrensverzeichnisses betreffen.

§ 1 Absatz 3 definiert, was unter einem neuen Verfahren oder einer wesentlichen Änderung eines bestehenden Verfahrens zu verstehen ist.

§ 1 Absatz 4 VerfVerzV enthält die Klarstellung, dass ein Verfahrensverzeichnis auch elektronisch geführt werden kann und dient der Verwaltungsvereinfachung, sofern die Daten verarbeitenden Stellen hiervon Gebrauch machen.

§ 2 Satz 1 VerfVerzV stellt klar, dass in den Fällen, in denen die zuständigen obersten Landesbehörden oder die von ihr bestimmte Stelle Verfahren auf der Grundlage von § 7 Absatz 3 Satz 5 BbgDSG freigeben, diese den Daten verarbeitenden Stellen die notwendigen Angaben für das Verfahrensverzeichnis zur Verfügung zu stellen haben.

Das heißt, den Daten verarbeitenden Stellen werden die Informationen beziehungsweise Festlegungen zur Verfügung gestellt, die durch die freigebende Stelle vorgegeben sind. Dies wird vor allem die Angaben zu den Nummern 3 bis 8 und 11 sowie gegebenenfalls der Nummer 9 betreffen. Lediglich dort, wo eigene Spielräume zur Verfahrensgestaltung bestehen, können und müssen die Daten verarbeitenden Stellen eigene Festlegungen treffen.

Eine entsprechende Verpflichtung zur Übermittlung regelt § 2 Satz 2 VerfVerzV bei von mehreren öffentlichen Stellen gemeinsam oder zentral betriebenen Verfahren für die Angaben bezüglich der zentral betriebenen Komponenten beziehungsweise Teilverfahren.

Durch § 3 Absatz 1 VerfVerzV wird klargestellt, dass die Einsichtnahme auch durch eine Veröffentlichung des Verfahrensverzeichnisses im Internet gewährleistet werden kann. Hierdurch können sich die anwendenden Stellen von Verwaltungsaufwand im Falle eines Einsichtsbegehrens entlasten. Nach einem Hinweis der LDA sind die Angaben zu § 8 Absatz 1 Nummer 8 und 9 BbgDSG nicht im Internet zu veröffentlichen, weil hierdurch potenzielle Angreifer Rückschlüsse auf möglicherweise vorhandene Sicherheitslücken ziehen könnten.

Nach § 3 Absatz 2 VerfVerzV muss die Daten verarbeitende Stelle die Gründe aufzeichnen, warum eine Einsichtnahme in die Angaben nach § 8 Absatz 1 Nummer 7 bis 11 BbgDSG die Sicherheit des Verfahrens beeinträchtigen würde. Hierdurch wird die ohnehin zu treffende Entscheidung über eine etwaige Nichtveröffentlichung nachvollziehbar dokumentiert. Es bedarf nicht bei jedem Einsichtsbegehren der erneuten Prüfung und gegebenenfalls Begründung der Entscheidung.

§ 4 VerfVerzV regelt das Inkrafttreten der Verordnung. Für neue Verfahren, die nach Inkrafttreten der VerfVerzV eingesetzt werden, ist ein Verfahrensverzeichnis auf der Grundlage der geänderten Verordnung zu erstellen. Eine Anpassung von Verzeichnissen zu bestehenden Verfahren muss erst bei einer wesentlichen Änderung des jeweiligen Verfahrens vorgenommen werden. Es wird jedoch empfohlen, eine Anpassung innerhalb von zwei Jahren nach Inkrafttreten der Verordnung vorzunehmen.

2 Ausfüllhinweise für das Musterformblatt

2.1 Vorbemerkung

Jede Stelle, die personenbezogene Daten selbst automatisiert verarbeitet oder im Auftrag verarbeiten lässt, hat für das dabei jeweils angewandte Verfahren die zugrunde liegenden wesentlichen datenschutzrechtlichen Aspekte in einem Verzeichnis darzustellen beziehungsweise festzulegen. Der Inhalt des Verzeichnisses ist in § 8 Absatz 1 BbgDSG geregelt. Der entsprechende Vordruck ist Anlage der Verfahrensverzeichnisverordnung und damit verbindlich vorgeschrieben.

Gemäß § 8 Absatz 5 BbgDSG ist die Erstellung eines Verfahrensverzeichnisses zum Beispiel nicht erforderlich für Verfahren, deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse geltend machen können, zur Einsichtnahme offen steht. Auch für Verfahren, mit denen Datensammlungen erstellt werden, die nicht länger als drei Monate vorgehalten werden, Registraturverfahren oder Verfahren, die unter Einsatz handelsüblicher Schreibprogramme ablaufen, muss kein Verzeichnis erstellt werden. Letzteres gilt jedoch nur dann, wenn über übliche Suchbefehle hinaus eine personenbezogene Auswertbarkeit nach bestimmten Kriterien (zum Beispiel durch entsprechende Auswertprogramme) nicht gegeben ist. So ist beispielsweise für eine Verarbeitung personenbezogener Daten unter Nutzung von Tabellenkalkulationsprogrammen in der Regel ein Verfahrensverzeichnis zu erstellen.

Das Verfahrensverzeichnis muss unter anderem eine allgemeine Beschreibung der eingesetzten Datenverarbeitungsanlagen und der verwendeten Software enthalten.

Besonderes Gewicht ist auf die Darstellung der technischen und organisatorischen Maßnahmen nach § 10 BbgDSG zu legen. § 10 BbgDSG wurde im Zuge der Novellierung des Datenschutzgesetzes im Jahr 2007 neu gefasst. Die Änderungen sind bei der Erstellung des Verfahrensverzeichnisses zu berücksichtigen. Die aufzuführenden Maßnahmen ergeben sich aus dem nach § 7 Absatz 3 Nummer 1 BbgDSG zu entwickelnden Sicherheitskonzept.

Soweit Verfahren zentral betrieben und von mehreren Daten verarbeitenden Stellen eingesetzt werden, wird für die zentral bereit gestellten Komponenten ein Verfahrensverzeichnis durch die für den zentralen Betrieb zuständige öffentliche Stelle geführt. Dieses ist, sofern erforderlich, den jeweiligen das Verfahren anwendenden beziehungsweise nutzenden Stellen zur Verfügung zu stellen (§ 2 Satz 2 VerfVerzV). Die das Verfahren nutzenden Daten verarbeitenden Stellen haben für ihren Verantwortungsbereich ebenfalls ein Verfahrensverzeichnis zu erstellen. Gegebenenfalls besteht das Verfahrensverzeichnis aus zwei Teilen, die die zentralen und dezentralen Komponenten abbilden. Ergänzend wird auf die Ausführungen zu § 1 Absatz 2 VerfVerzV (siehe oben) hingewiesen.

2.2 Zu den Angaben im Einzelnen:

- Daten verarbeitende Stelle

Hier ist die jeweilige Daten verarbeitende Behörde oder Einrichtung zu nennen, zum Beispiel das Ministerium X oder die Gemeinde Y. Die für das Verfahren fachlich verantwortliche Organisationseinheit innerhalb der öffentlichen Stelle wird unter Nummer 2 benannt.

- Regelungen zur Einsichtnahme

Bei der Erstellung des Verfahrensverzeichnisses ist auf der Grundlage von § 8 Absatz 4 BbgDSG die Entscheidung zu treffen, ob es vollständig, teilweise oder gar nicht zur Einsichtnahme durch jedermann offen steht. Sofern eine Veröffentlichung im Internet erfolgt, dürfen die Angaben zu § 8 Absatz 1 Nummern 8 und 9 BbgDSG nicht zugänglich gemacht werden, weil anderenfalls potenzielle Angreifer Rückschlüsse auf möglicherweise vorhandene Sicherheitslücken ziehen könnten.

Gemäß § 3 Absatz 2 VerfVerzV sind die Gründe für eine Beschränkung der Einsichtnahme aufzuzeichnen. Diese sollten aus Zweckmäßigkeitsgründen dem Verfahrensverzeichnis als Anlage beigefügt werden. Eine Veröffentlichung der Gründe für eine Beschränkung der Einsichtnahme erfolgt nicht.

- Nummer 1 - Bezeichnung des Verfahrens

Die Bezeichnung sollte die Zweckbestimmung des Verfahrens erkennen lassen. Gleichzeitig ist festzuhalten, ob es sich um den erstmaligen Einsatz oder eine wesentliche Änderung des Verfahrens handelt. Wesentlich ist eine Änderung dann, wenn eine erneute Freigabe nach § 7 Absatz 3 zu erteilen ist. Dies ist insbesondere dann der Fall, wenn sich die den Angaben zu den Nummern 3 bis 7 sowie 9 und 10 zugrunde liegenden Sachverhalte nicht nur marginal verändert haben.

- Nummer 2 - Verantwortliche Organisationseinheit

Diese Angabe soll verdeutlichen, welche Organisationseinheit innerhalb einer Behörde die fachliche Verantwortung für das Verfahren trägt. Es ist die Stelle anzugeben, die für die materielle Rechtmäßigkeit der Datenverarbeitung verantwortlich ist. Diese muss innerhalb einer Behörde nicht mit der Stelle identisch sein, die die Freigabe für das Verfahren erklärt. Anzugeben ist dabei nicht die Ordnungsnummer beispielsweise eines Referates, sondern die Aufgabe, zum Beispiel Personalreferat, Jugendamt, Ausländerbehörde.

Durch diese Angabe ändert sich nichts an der datenschutzrechtlichen Verantwortung der Daten verarbeitenden Stelle.

- Nummer 3 - Zweckbestimmung und Rechtsgrundlage

Unter „3.1 - Zweckbestimmung“ sind alle Zwecke so konkret wie möglich zu nennen, zu denen die Verarbeitung personenbezogener Daten erfolgt. Begrenzt werden die zulässigen Zwecke durch die gesetzliche Aufgabenzuweisung beziehungsweise eine etwaige Einwilligungserklärung.

Unter „3.2 - Rechtsgrundlage“ ist die Ermächtigung für die Datenverarbeitung anzugeben.

Dabei ist die konkrete Rechtsnorm anzugeben, auf deren Grundlage die Verarbeitung personenbezogener Daten erfolgt. Ein allgemeiner Bezug zum Beispiel auf das SGB II reicht nicht aus. Es ist unter Angabe der zugrunde liegenden Rechtsnorm die spezifische Aufgabe zu benennen, der das Verfahren dient (zum Beispiel Bearbeitung von Anträgen auf Wohngeld nach dem Wohngeldgesetz, Bearbeitung von Anträgen auf Ausstellung eines Reisepasses).

- Nummer 4 - Betroffene Personengruppen und die diesbezüglichen Daten und Datenkategorien

Unter „4.1 - Kreis der Betroffenen“ sollen die Personen/-gruppen, deren Daten verarbeitet werden, so konkret wie möglich benannt werden, zum Beispiel „Personen, die einen Antrag auf … gestellt haben“ oder „Kinder der Antragsteller“. Die Zahl der möglichen Betroffenen kann aufgrund von Erfahrungswerten geschätzt werden. Ist eine Schätzung nicht möglich, kann die Angabe unterbleiben.

Unter 4.2 ist die Art der gespeicherten Daten oder Datenkategorien anzugeben, zum Beispiel Personen-, Sach- oder Falldaten. Diese sind soweit wie möglich zu konkretisieren. Hierbei ist auch anzugeben, ob es sich dabei um die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 4a BbgDSG handelt. Sofern solche Daten verarbeitet werden sollen, ist an die Notwendigkeit der Vorabkontrolle gemäß § 10a BbgDSG zu denken.

- Nummer 5 - Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden

Unter Bezugnahme auf die Angaben zu Nummer 4 ist für jede Datenkategorie der Empfänger oder die Kategorien von Empfängern festzulegen. Dies betrifft die Empfänger, an die eine Mitteilung personenbezogener Daten bereits im Verfahren angelegt ist, also regelmäßig erfolgt.

Empfänger ist jede Person oder Stelle, die Daten erhält (§ 4 Absatz 4 Nummer 2 BbgDSG). Das heißt, hier sind auch Stellen innerhalb einer Behörde anzugeben, wenn diese personenbezogene Daten erhalten. Nicht anzugeben sind in dem Verfahrensverzeichnis Stellen, an die grundsätzlich keine Mitteilung vorgesehen ist, es aber dennoch auf Grund besonderer Fallkonstellation beziehungsweise auf der Grundlage spezieller Rechtsvorschriften zu einer Datenweitergabe kommen kann. Dies kann beispielsweise die Übermittlung an Polizeibehörden oder aber an Dritte, aufgrund eines rechtlichen Interesses des Dritten, betreffen, soweit die speziellen Voraussetzungen dafür vorliegen.

- Nummer 8 - Fristen für die Sperrung/Löschung der Daten (§ 19 BbgDSG)

Es ist festzulegen, innerhalb welcher Fristen regelmäßig eine Prüfung erfolgt, ob die Daten weiterhin zur Aufgabenerfüllung gemäß § 13 BbgDSG beziehungsweise der bereichsspezifischen Norm erforderlich sind oder eine Löschung oder Sperrung gemäß § 19 BbgDSG notwendig ist.

Sofern die der automatisierten Datenverarbeitung zugrunde liegende Rechtsvorschrift eine spezielle Löschungsvorschrift enthält, ist diese Frist unter Bezugnahme auf die Rechtsvorschrift als regelmäßige Löschungsfrist anzugeben.

- Nummer 9 - Kurzbeschreibung der technischen und organisatorischen Maßnahmen gemäß § 10 Absatz 2 BbgDSG

Die konkreten Maßnahmen ergeben sich aus dem Sicherheitskonzept nach § 7 Absatz 3 BbgDSG. Hier ist nur eine kurze Beschreibung vorzunehmen, die eine überschlägige Beurteilung

der Angemessenheit der Maßnahmen in Bezug auf die mit dem Verfahren verbundenen Gefährdungen zulässt. Erläuternd wird hierzu auf die einzelnen Schutzziele der technischen und organisatorischen Maßnahmen hingewiesen:

- Gewährleistung von Vertraulichkeit

Vertraulichkeit ist dann gewährleistet, wenn die gespeicherten Daten nicht in die Hände Unbefugter geraten können. Dieses Ziel kann durch verschiedene Maßnahmen erreicht werden. In Betracht kommen die Festlegung von Modalitäten zur Benutzeridentifikation und -autorisierung. Dies kann durch die Vergabe von Benutzername und Passwort, aber auch durch die Nutzung von Chipkarten und PIN erfolgen. Des Weiteren ist ein Berechtigungskonzept notwendig, damit Nutzer nur auf die tatsächlich benötigten Daten zugreifen können. Zu denken ist auch an die sichere Aufbewahrung oder Unterbringung der verwendeten Hardware und Backup-Datenträger, die Nutzung von Verschlüsselungssoftware bei der Speicherung in unsicheren Umgebungen (zum Beispiel Notebook, Laptop, lokaler PC) oder besonders sensitiver Daten in Datenbanken und bei der Datenübertragung in Netzwerken oder die vertrauliche Behandlung von Angaben über verwendete Hard- und Software und die Systemkonfiguration.

- Gewährleistung von Integrität

Integrität ist gewährleistet, wenn die Datenbestände unversehrt, vollständig und aktuell sind, also verlässlich richtig. Integrität muss während aller Phasen der Datenverarbeitung von der Erhebung bis zur Sperrung/Löschung gegeben sein (§ 3 Absatz 2 BbgDSG). Unter anderem muss gewährleistet sein, dass Daten nicht durch Computerviren oder andere Schadsoftware verfälscht werden.

- Gewährleistung von Verfügbarkeit

Verfügbarkeit bedeutet, dass die Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können. Die Verfügbarkeit bezieht sich nicht nur auf die gespeicherten personenbezogenen Daten, sondern gleichermaßen auf die Hardware und die zur Verarbeitung erforderlichen Programme. Das Datenverarbeitungssystem ist hinsichtlich der Verfügbarkeit in seiner Gesamtheit zu betrachten.

- Gewährleistung von Authentizität

Die Authentizität ist dann gewährleistet, wenn ein Dokument beziehungsweise Datum zweifelsfrei seinem Ursprung zugeordnet werden kann.

Die Gewährleistung der Authentizität ist hauptsächlich bei elektronisch übertragenen Daten von Bedeutung. Den Gefährdungen kann durch Verfahren begegnet werden, bei denen die Herkunft der Daten nachvollziehbar ist. Bei der Bewertung der Verfahren sind verwendete Hardwarekomponenten und Programme einzubeziehen, zum Beispiel beim E-Government oder beim elektronischen Zahlungsverkehr. Beispiel: Einsatz von Signaturverfahren, bei denen rechtsverbindlich festgestellt werden kann, ob die Daten von den Betroffenen autorisiert (zum Beispiel digital signiert) worden sind oder wer der Urheber von Daten ist, die nicht von den Betroffenen stammen (zum Beispiel bei Datenübermittlung).

- Gewährleistung von Revisionsfähigkeit

Revisionsfähigkeit bedeutet, dass nachprüfbar ist, wie Daten in einen Datenbestand gelangt sind und welche Veränderungen sie im Laufe der Zeit durch wen erfahren haben. Nachprüfbar muss sein, wer für das Aufnehmen bestimmter Daten in einen Datenbestand oder ihr Entfernen daraus die Verantwortung trägt. Dies kann durch entsprechende Protokolldateien gewährleistet werden, die jedoch selbst ein datenschutzrechtliches Risiko bergen und deshalb einer engen Zweckbindung nach § 29 Absatz 4 BbgDSG unterliegen.

- Gewährleistung von Transparenz

Zur Herstellung von Transparenz sind automatisierte Verfahren in aktueller Form nachvollziehbar zu dokumentieren. Die einzelnen Verfahrensschritte müssen dabei so beschrieben werden, dass die Systematik der Prozesse ohne erheblichen zusätzlichen Aufwand nachvollziehbar wird. Transparenz wird vor allem durch die Dokumentation der Freigabe oder der Vorabkontrolle nach § 7 Absatz 3 BbgDSG, das ordnungsgemäße Führen des Verfahrensverzeichnisses sowie der Dokumentation von wesentlichen Programmänderungen beziehungsweise die laufende Fortschreibung der Programmdokumentation hergestellt.

- Nummer 10 - Allgemeine Beschreibung der eingesetzten Datenverarbeitungsanlagen

Unter diesem Punkt sollen die zur Datenverarbeitung eingesetzten Anlagen und deren Zusammenwirken beschrieben werden. Des Weiteren ist die verwendete Software zu nennen. Die Angaben sind der Risikoanalyse beziehungsweise dem Sicherheitskonzept zu entnehmen.

- Nummer 11 - Freigabeerklärung

Gemäß § 7 Absatz 3 BbgDSG ist für jedes Verfahren, für das ein Verfahrensverzeichnis nach § 8 BbgDSG zu erstellen ist, die Freigabe zu erklären. Welche Organisationseinheit innerhalb einer Daten verarbeitenden Stelle die Freigabe erklärt, unterliegt der Organisationshoheit der jeweiligen Daten verarbeitenden Stelle. Dies muss nicht zwangsläufig die Organisationseinheit sein, die die fachliche Verantwortung für die (materielle) Rechtmäßigkeit des Verfahrens trägt. Aufgrund der Komplexität der nach § 10 BbgDSG zu treffenden technischen Maßnahmen kann die Freigabe - gegebenenfalls nach Bestätigung der materiellen Rechtmäßigkeit durch die fachlich zuständige Organisationseinheit - beispielsweise auch durch die für die Informationstechnik zuständige Organisationseinheit erfolgen. In jedem Fall ist die Fachebene in das Freigabeverfahren einzubeziehen.

Soweit Verfahren zentral betrieben und von mehreren Daten verarbeitenden Stellen eingesetzt werden, erfolgt eine Freigabe jeweils für den Verantwortungsbereich der einzelnen Daten verarbeitenden Stelle. Das heißt, für zentral betriebene Komponenten erfolgt eine Freigabe durch die hierfür verantwortliche Stelle; für dezentrale Komponenten erfolgt die Freigabe durch die jeweilige Daten verarbeitende Stelle auf dezentraler Ebene.

Vor der Freigabe kann gegebenenfalls das Votum des behördlichen Datenschutzbeauftragten eingeholt werden. Sofern Verfahren der Vorabkontrolle unterliegen, ist dieser ohnehin zu beteiligen.

Die Freigabeerklärung sowie das Ergebnis einer gegebenenfalls vorzunehmenden Vorabkontrolle sind dem Verfahrensverzeichnis als Anlage beizufügen.

VV-BbgDSG
Anlage 2 zu den Nummern 13.5 und 14.2

Mindestvertragsinhalt für Verträge nach § 11 BbgDSG

1. In einer schriftlichen Vereinbarung sind (gegebenenfalls in einem Abschnitt Datenschutz/Datensicherung) mindestens folgende Regelungen zu treffen:

   a) Gegenstand und Dauer des Auftrages;

   b) Art und Umfang des Umgangs mit den Daten (insbesondere konkrete Angaben zu den einzelnen Phasen der Datenverarbeitung, den verwendeten Anlagen, Systemen und Programmen);

   c) die nach § 10 BbgDSG zu treffenden technischen und organisatorischen Maßnahmen, insbesondere:

      - Zeitpunkt, Ort, Protokollierung und Berechtigte für die Anlieferung und Ausgabe der zu verarbeitenden Daten
      - Versandform und Transport
      - Art und Aufbewahrung der Datenträger (Belege, Filme und Ähnliches) beim Auftragnehmer
      - Maßnahmen zur Entsorgung von Fehldrucken oder Ausschussmaterial
      - Maßnahmen bei Verlust von Datenträgern;

   d) Vereinbarungen über die Verfahrensabnahme und Programmfreigabe und gegebenenfalls zur Unterstützung bei der Erstellung des Verfahrensverzeichnisses nach § 8 BbgDSG;

   e) unverzügliche Mitteilung des Auftragnehmers an den Auftraggeber über eingetretene Veränderungen in oben genannten Punkten;

   f) Umfang der Weisungsbefugnisse des Auftraggebers;

   g) die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen (gegebenenfalls nur mit Genehmigung des Auftraggebers);

   h) Art der Gewährleistung der Kontrolle des Umgangs mit den Daten und der Datenschutzmaßnahmen durch den Auftraggeber (Zutritt zu Räumen, Einsicht in Anlagen);

   i) Verpflichtung des Auftragnehmers, den Auftraggeber unverzüglich über alle Verstöße gegen bestehende Datenschutzbestimmungen beim Umgang mit den Daten oder bei Weisungen des Auftraggebers zum Umgang mit den Daten zu unterrichten;

   j) Vereinbarung der fristlosen Kündigung bei Verletzungen von Datenschutz-/Datensicherheitsmaßnahmen;

   k) Rückgabe überlassener Datenträger und Daten, sowie Löschung der beim Auftragnehmer gespeicherten Daten nach Vertragsende.

2. Ist der Auftragnehmer eine private Stelle oder ein öffentlich-rechtliches Wettbewerbsunternehmen, sind zusätzlich folgende Punkte vertraglich zu regeln:

   a) Verpflichtung des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen und sich ausschließlich an dessen Weisungen zu halten;

   b) Verpflichtung des Auftragnehmers, vom Auftraggeber veranlasste Kontrollen zu ermöglichen;

   c) Verpflichtung aller Mitarbeiter des Auftragnehmers, die Zugang zu den Daten haben, auf das Datengeheimnis (gemäß § 5 BDSG);

   d) regelmäßige Kontrolle des Umgangs mit den Daten durch den Datenschutzbeauftragten des Auftragnehmers (betrieblicher Datenschutzbeauftragter nach dem Bundesdatenschutzgesetz).

Ergänzend wird auf § 11 des Bundesdatenschutzgesetzes (insbesondere auf dessen Absatz 2) verwiesen.

VV-BbgDSG
Anlage 3 zu Nummer 14.2

Mindestvertragsinhalt für Wartungsverträge nach § 11a BbgDSG

Hinsichtlich des Inhalts des Vertrages sind die Verwaltungsvorschriften zu § 11 entsprechend anzuwenden. Darüber hinaus sind folgende spezielle Regelungen zu treffen:

1. Bestimmungen hinsichtlich der Abgrenzung der Rechte und Pflichten zwischen Auftraggeber und Auftragnehmer;

2. eine Protokollierungspflicht über die Arbeiten beim Auftraggeber;

3. Regelungen, dass die Daten ausschließlich für den Zweck der Wartung verwendet werden dürfen;

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

5. nach Abschluss der Wartungsarbeiten sind eventuell beim Auftragnehmer vorhandene Daten zu löschen;

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

7. die Anwesenheit des Systemverwalters ist sicherzustellen;

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

9. für den Fall, dass der Auftragnehmer eine Stelle nach § 17 Absatz 2 BbgDSG ist, sind stets die hierfür geltenden Regelungen zur Übermittlung personenbezogener Daten anzuwenden.

VV-BbgDSG
Anlage 4 zu Nummer 14.3

Anforderungskatalog zu § 11a Absatz 1 BbgDSG

Werden Datenverarbeitungssysteme vor Ort oder über Datenfernübertragungseinrichtungen (Fernwartung) gewartet, so sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

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 können;

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.