

Dienstanweisung Nr. 22 / 96

Datenschutz und Datensicherheit beim Umgang mit personenbezogenen Daten

Inhaltsverzeichnis:

- 1. Grundlagen
 - 1.1. Gesetzliche Grundlagen
 - 1.2. Das Recht der informationellen Selbstbestimmung
 - 1.3. Geltungsbereich
- 2. Organisation des Datenschutzes
 - 2.1. Personell
 - 2.1.1. Landrat
 - 2.1.2. Amtsleiter
 - 2.1.3. Behördlicher Datenschutzbeauftragter
 - 2.2. Organisatorisch
 - 2.2.1. Begriffsbestimmungen zu Datenschutz und Datenverarbeitung
 - 2.2.2. Rechte der Betroffenen
 - 2.2.3. Sicherung des Datengeheimnisses
 - 2.2.4. Sicherstellung des Datenschutzes
 - 2.2.4.1. Festlegung der Schutzstufen
 - 2.2.4.2. Sachgebiet Automatisierte Datenverarbeitung (ADV)
 - 2.2.4.3. Fachamt
 - 2.2.4.4. Datenschutzbeauftragter
 - 2.2.4.5. Personalrat
 - 2.3. Technisch
- 3. Inkrafttreten

1. Grundlagen

1.1. Gesetzliche Grundlagen

Als allgemeine Rechtsvorschriften für den Datenschutz sind anzuwenden:

Das Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954) zuletzt geändert durch Artikel 12 Abs. 16 des Postneuordnungsgesetzes vom 14. September 1994 (BGBl. I S. 2385), sowie das Brandenburgische Datenschutzgesetz (Bbg DSG) vom 20. Januar 1992 (Gesetz- und Verordnungsblatt für das Land Brandenburg 1992 Teil I Nr. 1 S. 2 in der Fassung des ersten Gesetzes zur Änderung des Bbg DSG vom 08. Februar 1996 (Gesetz- und Verordnungsblatt für das Land Brandenburg 1996 Teil 1 Nr. 3 S. 17 ff).

Soweit andere Rechtsvorschriften auf die Verarbeitung personenbezogener Daten anzuwenden sind, gehen diese den Vorschriften der vorgenannten Gesetze vor (BDSG § 1 (4), BbgDSG § 2 (3)). Dies betrifft nicht das Verwaltungsverfahrensgesetz (BDSG § 1 (5), Bbg DSG § 2 (3)).

1.2. Das Recht der informationellen Selbstbestimmung

Eine starke Sensibilisierung für die Belange des Datenschutzes wurde durch das "Volkszählungsurteil" des Bundesverfassungsgerichtes (BVerfG, Urteil vom 15. Dezember 1983) erreicht.

Darin wird ausgeführt:

"Aus dem allgemeinen Persönlichkeitsrecht folgt das Recht des Einzelnen grundsätzlich selbst zu entscheiden, wann und in welchem Umfang andere von seinen persönlichen Lebenssachverhalten erfahren ("informationelle Selbstbestimmung")."

Das Recht auf informationelle Selbstbestimmung gewährleistet somit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Ausnahme:

Einschränkungen, die im überwiegenden Allgemeininteresse erfolgen, hat der Einzelne grundsätzlich hinzunehmen.

Bedingung für die Ausnahme:

Es muss eine gesetzliche Grundlage vorhanden sein, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben.

1.3. Geltungsbereich

Diese Dienstanweisung ist allgemeingültig für alle Mitarbeiter der Kreisverwaltung des Landkreises Teltow-Fläming.

Erforderliche spezielle Anweisungen werden gesondert erlassen und regeln Sonderfälle für einzelne Arbeitsbereiche, jedoch nicht unter Verletzung dieser Dienstanweisung oder Teilen davon.

2. Organisation des Datenschutzes

2.1. Personell

2.1.1. Landrat

Verantwortlich für die Einhaltung und Durchführung des Datenschutzes in der Kreisverwaltung ist der Landrat.

2.1.2. Amtsleiter

Den Amtsleitern obliegt die vorgenannte Verantwortung für ihr Amt. Bei ämterübergreifenden Vorgängen ist die gemeinsame Verantwortung aller beteiligten Amtsleiter gegeben und wahrzunehmen.

Bei Bedarf gibt es Abstimmungsgespräche zwischen dem Datenschutzbeauftragten, den Amtsleitern und den ADV-Verantwortlichen. Im Ergebnis erfolgt eine protokollarische Festlegung der Verantwortlichkeit.

2.1.3. Behördlicher Datenschutzbeauftragter

Der Landrat bestellt für die Kreisverwaltung einen behördlichen Datenschutzbeauftragten. Dieser ist in der Durchführung seiner Aufgabe weisungsfrei und nur dem Landrat unterstellt. Er ist Ansprechpartner zu allen Fragen des Datenschutzes und wird beratend, koordinierend, kontrollierend und entscheidungsvorbereitend tätig.

Er ist in seiner Aufgabe nicht weisungsbefugt.

Nach Beauftragung durch den Landrat setzt der Datenschutzbeauftragte datenrelevante Festlegungen, die der Zustimmung des Landrates bedürfen, bei den Amtsleitern durch.

2.2. Organisatorisch

2.2.1. Begriffsbestimmungen zu Datenschutz und Datenverarbeitung

Diese sind im § 3 des Bbg DSG erläutert.

Siehe dazu

-Anlage 1-

2.2.2. Rechte des Betroffenen

Diese sind im § 5 des Bbg DSG erläutert. Damit im Zusammenhang stehen außerdem die §§ 18, 19, 20 und 21 des Bbg DSG.

Siehe dazu

- Anlage 2-

Alle Anfragen Betroffener sind unmittelbar und unverzüglich dem Datenschutzbeauftragten zuzuleiten. Dieser veranlasst die Bearbeitung und Beantwortung.

Dafür erforderliche Zuarbeiten werden über die Amtsleiter angefordert und sind kurzfristig und unverzüglich zu leisten.

2.2.3. Sicherung des Datengeheimnisses

Alle Mitarbeiter, die dienstlichen Umgang mit personenbezogenen Daten haben, werden entsprechend § 6 Bbg DSG durch den Amtsleiter auf das Datengeheimnis verpflichtet.

Diese Verpflichtung erfolgt schriftlich in 2-facher Ausfertigung. Verteiler der Verpflichtung: Personalakte, Verpflichteter.

Der Datenschutzbeauftragte erhält vom Hauptamt eine aktuelle Übersicht aller Verpflichteten nach Stellen des Stellenplanes.

Muster der Verpflichtung

- Anlage 3-

2.2.4. Sicherstellung des Datenschutzes

Geregelt in § 7 Bbg DSG. Damit im Zusammenhang stehen weiterhin die §§ 8, 9, 10 und 11 des Bbg DSG.

Siehe dazu

- Anlage 4 -

2.2.4.1. Festlegung der Schutzstufen

Die Festlegungen zum Umgang mit personenbezogenen Daten sind immer anhand des konkreten Falles unter Berücksichtigung der Schutzbedürftigkeit der Daten zu treffen. Aus diesem Grund erfolgt die Einteilung der Schutzbedürftigkeit in vier Schutzstufen. Für gleiche Schutzstufen sind gleiche bzw. gleichwertige Maßnahmen festzulegen.

Die Klassifizierung erfolgt nach folgenden 4 Schutzstufen:

Stufe A:

personenbezogene Daten, deren Missbrauch im Allgemeinen keine besondere Beeinträchtigung schutzwürdiger Belange des Betroffenen erwarten lässt (Repräsentation)

Erläuterung: Daten, die nicht allgemein zugänglich sind (internes Schriftgut). Die Kenntnisnahme ist an ein berechtigtes Interesse des Einsichtnehmenden gebunden.

Beispiele: einfache Melderegisterauskunft, soweit sie zulässig ist; Dateien, die Adressangaben (Name, Anschrift, Telefonnummer), Berufs-, Dienst-, Amts-, Branchen- oder Geschäftsbezeichnungen und akademische Grade enthalten

Umgang mit diesen Daten unter Beachtung der Erläuterung:

Vervielfältigung	- keine Beschränkung
Zugang/Weitergabe intern	- keine Beschränkung
Weitergabe extern	- in Absprache mit dem Vorgesetzten
Transport intern	- einfacher Hauspostumschlag
Transport extern	- Standardbrief
Aufbewahrung	- Büromöbel (Brandschutz)
Entsorgung	- über Aktenvernichter durch Entsorgungsunternehmen

Stufe B:

personenbezogene Daten, deren Missbrauch den Betroffenen in seiner gesellschaftlichen Stellung oder seinen wirtschaftlichen Verhältnissen beeinträchtigen kann (Ansehen)

Erläuterung: vertrauliche Daten

Beispiele: Mietverhältnisse, Geschäfts- und Vertragsbeziehungen, Familienstand und verwandtschaftliche Beziehungen, Bekanntenkreis, Ausbildung, Wehrdienstzeit, Zugehörigkeit zu Verbänden und Vereinen, Zugehörigkeit zu gesetzlichen und privaten Versicherungen einschließlich der Beiträge

Umgang mit diesen Daten unter Beachtung der Erläuterung:

Vervielfältigung	- Genehmigung nach pflichtgemäßem Ermessen des Dateiverantwortlichen
Zugang/Weitergabe intern	- nur für Mitarbeiter, die diese Daten zur Erfüllung übertragener Aufgaben benötigen oder zur Kenntnis erhalten müssen Das bedeutet: persönliche Informationen über Dienstausswertungen dürfen nicht offen in den Verteilerkästen der Sekretariate liegen.
Weitergabe extern	- nur im Rahmen datenschutzrechtlicher Zulässigkeitstatbestände erlaubt
Transport intern	- einfacher Hauspostumschlag oder verschlossener Umschlag - nach Ermessen des Absenders
Transport extern	- Standardbriefe
Aufbewahrung	- Verschluss in Büromöbeln Während des Tages so aufbewahren, dass Unbefugte keinen Einblick haben.
Entsorgung	- über Aktenvernichter durch Entsorgungsunternehmen

Stufe C:

personenbezogene Daten, deren Missbrauch die gesellschaftliche Stellung und die wirtschaftlichen Verhältnisse des Betroffenen erheblich beeinträchtigen kann bzw. die einem Berufs- oder besonderen Amtsgeheimnis unterliegen (moralische und soziale Existenz)

Erläuterung: geheime Daten

Beispiele: gesundheitliche Verhältnisse (gegenwärtige und vergangene), besonders sensible Patientendaten, strafbare Handlungen, religiöse oder politische Anschauungen (Zugehörigkeit zu Parteien, Gewerkschaften, politischen oder religiösen Verbänden und Vereinen), Prüfungs- und Schulzeugnisse, Zugehörigkeit zu Krankenkassen einschließlich Beiträge, arbeitsrechtliche Verhältnisse, Disziplinarverfahren, Ordnungswidrigkeiten, Verwarnungen, Steuerdaten, Sozialdaten, psychologische Daten, Unterbringung in Anstalten, Adoptionen, Betreuungen, Wahlausschlüsse, Passversagen, besondere Daten des Melderegisters

Umgang mit diesen Daten unter Beachtung der Erläuterungen:

Vervielfältigung	- Datenempfänger darf diese ohne Genehmigung des Herausgebers nicht vervielfältigen
Zugang/Weitergabe intern	- nur für Mitarbeiter, die diese Daten zur Erfüllung übertragener Aufgaben benötigen oder zur Kenntnis erhalten müssen. Das bedeutet: persönliche Information über Dienstausschwertungen dürfen nicht offen in den Verteilerkästen der Sekretariate liegen.
Weitergabe extern	- nur im Rahmen datenschutzrechtlicher Zulässigkeitstatbestände erlaubt
Transport intern	- Umschlag mit Vermerk "persönlich" oder persönliche Übergabe nach Ermessen des Absenders
Transport extern	- Einschreiben oder Wertsendung mit Rückschein oder Kurierdienst
Aufbewahrung	- Verschluss in Büromöbeln mit besonders gesicherten Behältnissen oder im Tresor Während des Tages so aufbewahren, dass Unbefugte keinen Einblick haben.
Entsorgung	- Durch Entsorgungsunternehmen über schriftlichen Vertrag als Datenverarbeitung im Auftrag gemäß Sicherheitsstufe S 4 nach DIN 32757 Siehe dazu - Anlage 6-

Stufe D:

personenbezogene Daten, deren Missbrauch die Gesundheit, Leib und Leben oder die Freiheit des Betroffenen erheblich beeinträchtigen kann (physische Existenz)

Erläuterung: streng geheime Daten

Beispiele: Adressen von Personen, die dem Zeugenschutzprogramm unterliegen,
Adressen von polizeilichen V-Leuten,
Melderegistersperren aus Gründen der Gefährdung von Leib und Leben.

Umgang mit diesen Daten unter Beachtung der Erläuterung:

Vervielfältigung	- nicht gestattet
Zugang/Weitergabe	- stark reduziert (eventuell Dienstherr)
Weitergabe extern	- bei staatlichen Offenbarungspflichten
Transport intern	- Versiegelung, persönliche Übergabe
Transport extern	- persönliche Übergabe, Sicherheitsfirma
Aufbewahrung	- Tresor, der besondere Sicherheitsanforderungen erfüllt
Entsorgung	- persönlich über Aktenvernichter

2.2.4.2 Sachgebiet ADV

Der erstmalige Einsatz automatisierter Verfahren zur Verarbeitung personenbezogener Daten, wesentliche Änderungen dazu, sowie Verarbeitung personenbezogener Daten im Auftrag werden unter Federführung des Sachgebietes ADV realisiert.

Mit der Aufgabenstellung zur Einführung bzw. Änderung von automatisierten Verfahren zur Verarbeitung personenbezogener Daten besteht für das Sachgebiet ADV die Verpflichtung zur umfassenden Einbeziehung, Information und Zusammenarbeit mit den betroffenen Fachämtern sowie dem Datenschutzbeauftragten.

Diese Einbeziehung, Information und Zusammenarbeit sind bis zur Einführung des Verfahrens bzw. der Änderungen kontinuierlich und konsequent weiterzuführen.

Zu allen Verfahren ist eine gute, übersichtliche Dokumentation zu erstellen, die für einen sachverständigen Dritten verständlich ist. Dieser muss damit in die Lage versetzt werden, sich einen ausreichenden Einblick in Aufbau, Ablauf und Arbeitsweise des DV - Verfahrens zu verschaffen.

Durch das Sachgebiet ADV wird eine allgemeingültige Dienstanweisung zu Fragen der ADV erarbeitet und ständig aktualisiert. Diese hat neben allgemeingültigen Festlegungen zur ADV auch allgemeingültige Festlegungen zum Datenschutz zu enthalten, die in dieser Anweisung nicht enthalten sind.

Weiterhin leistet das Sachgebiet ADV Zuarbeiten allgemeiner und spezifischer Art für die Fachämter. Diese Zuarbeiten werden durch die Fachämter abgefordert und haben die Erfordernisse zur Erarbeitung amtsspezifischer Regelungen zur ADV, zum Datenschutz und zur Datensicherheit zum Inhalt.

Der Datenschutzbeauftragte ist in allen Fällen zu beteiligen.

Das Sachgebiet ADV erstellt und führt das Geräteverzeichnis und stellt dem Datenschutzbeauftragten ein aktuelles Duplikat zur Verfügung.
Im Sachgebiet ADV liegen alle freigegebenen Dateibeschreibungen vor. Ein Duplikat erhält der Datenschutzbeauftragte.

Alle Anfragen zum Datenschutz beim Umgang mit personenbezogenen Daten sind unverzüglich dem Datenschutzbeauftragten zur Kenntnis zu geben. Dieser legt in Abstimmung mit dem Sachgebietsleiter die Verfahrensweise zur Beantwortung fest.

2.2.4.3. Fachamt

Sollte im Ausnahmefall ein Fachamt eigenständig automatisierte Verfahren zur Verarbeitung personenbezogener Daten erstmalig einsetzen, ändern oder Datenverarbeitung im Auftrag durchführen lassen wollen, so gelten die Aussagen unter 2.2.4.2. entsprechend.

Das Fachamt gilt als "datenverarbeitende Stelle" für die speziellen, fachamtsbezogenen ADV-Verfahren. Damit obliegt dem Fachamt die Federführung bei der Erarbeitung der Dateibeschriftung sowie der schriftlichen Dateifreigabe. Erarbeitung und Freigabe sind in enger Zusammenarbeit mit dem Sachgebiet ADV sowie dem Datenschutzbeauftragten vorzunehmen. Die Dateibeschriftung erhält das Sachgebiet ADV sowie als Duplikat der Datenschutzbeauftragte.

Für das Fachamt sind Regelungen (Dienstanweisungen o.ä.) zum Datenschutz und zur Datensicherheit beim Umgang mit personenbezogenen Daten zu erarbeiten. Diese sind auf die spezielle Problematik des Amtes, des Verfahrens sowie zu beachtender Schutzstufen zu beziehen und sind somit nicht in dieser sowie der Dienstanweisung ADV enthalten. Die Erarbeitung der Regelungen erfolgt durch den Datenschutzbeauftragten. Durch ihn werden die erforderlichen Zuarbeiten vom jeweiligen Amtsleiter und dem Sachgebiet ADV abgefordert.

Nach Abstimmung mit den eben genannten Beteiligten erfolgt die Inkraftsetzung. Alle genannten Beteiligten erhalten ein Exemplar dieser Regelungen.

Die gleiche Verfahrensweise gilt auch für die Verarbeitung in nicht-automatisierten Dateien, Akten, Bilddokumenten u.ä..

Die Einhaltung dieser Regelungen ist durch das Amt nachweislich zu überwachen. Festgestellte Verstöße sind dem Datenschutzbeauftragten mitzuteilen unter Beifügung eines Vorschlages, wie Abhilfe geschaffen werden soll.

Alle Anfragen zum Datenschutz beim Umgang mit personenbezogenen Daten sind unverzüglich dem Datenschutzbeauftragten zur Kenntnis zu geben. Dieser legt in Abstimmung mit dem jeweiligen Amtsleiter die Verfahrensweise zur Beantwortung fest.

2.2.4.4. Datenschutzbeauftragter

Der Datenschutzbeauftragte informiert, überwacht und berät zu allen Fragen des Datenschutzes die Kreisverwaltung betreffend.

10

Wichtig für die Erfüllung dieser Aufgabe ist die vertrauensvolle, kooperative und umfassende Zusammenarbeit mit den Ämtern, dem Sachgebiet ADV, der Verwaltungsleitung und dem Personalrat.

Aus diesem Grund werden alle eben genannten dazu verpflichtet, den Datenschutzbeauftragten rechtzeitig und umfassend über alle Vorhaben, die die Einführung oder wesentliche Änderung von Verfahren zur Verarbeitung von personenbezogenen Daten (automatisiert, nicht-automatisiert, über Akten o. ä.) betreffen zu unterrichten und ihn bis zur Einführung des Verfahrens ständig umfassend einzubeziehen.

Dem Datenschutzbeauftragten sind alle zur Erfüllung seiner Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen.

Er kann im Rahmen seiner Aufgabenerfüllung Zutritt zu den datenschutzrelevanten Stellen verlangen, soweit gesetzliche Regelungen dem nicht entgegenstehen. Im Zweifelsfall entscheidet der Landrat über die Verfahrensweise.

2.2.4.5. Personalrat

Eine frühzeitige Einbeziehung des Personalrates gemäß Personalvertretungsgesetz für das Land Brandenburg (Pers VG) §§ 60 (5); 65 Nr. 1 bis 5; 66 Nr. 13; 68 (3) Nr. 1

siehe Anlage 5

wird durch die Verwaltungsleitung gewährleistet.

Fragen der Schweigepflicht sowie die Löschung personenbezogener Daten in Akten oder Datenträgern des Personalrates sind geregelt in den §§ 10 und 94 (3) PersVG.

siehe ebenfalls Anlage 5

2.3. Technisch

Technische Maßnahmen zur Gewährleistung des Datenschutzes werden in der Anweisung zur Anwendung der ADV bzw. in den ämterspezifischen Regelungen festgelegt.

Geregelt werden sollten in diesem Zusammenhang folgende Fragen:

- Zugangskontrollen
- Brandschutzmaßnahmen
- Außenhautsicherung
- Datenträgeraufbewahrung
- Datenträgervernichtung
- Maßnahmen zur Betriebssicherung
- Verschlüsselung
- Backup - Planung

3. Inkrafttreten

Diese Dienstanweisung tritt ab 01.10.1996 in Kraft.

Luckenwalde, 04.09.1996

Giesecke
Landrat

Anlage -1-
zur Dienstanweisung Nr. 22/96

Zu Punkt 2.2.1.

Auszug aus dem Bbg DSG

§ 3 Bbg DSG

Begriffsbestimmungen:

- (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
- (2) Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Im Einzelnen ist
 - 1. Erheben (Erhebung) das Beschaffen von Daten über den Betroffenen.
 - 2. Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung.
 - 3. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten.
 - 4. Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die datenverarbeitende Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden oder dass der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten abrufen.
 - 5. Sperren (Sperrung) das Verhindern weiterer Verarbeitung gespeicherter Daten.
 - 6. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten.
 - 7. Nutzen (Nutzung) jede sonstige Verwendung personenbezogener Daten, ungeachtet der dabei angewendeten Verfahren.
- (3) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(4) Im Sinne dieses Gesetzes ist

1. datenverarbeitende Stelle jede öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt;
2. Dritter jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene sowie diejenigen Personen und Stellen, die im Inland personenbezogene Daten im Auftrag verarbeiten;
3. eine Datei eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, ungeordnet und ausgewertet werden kann (nicht-automatisierte Datei);
4. eine Akte jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger, soweit sie nicht Dateien im Sinne von Nr. 3 sind; nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorganges werden sollen und alsbald vernichtet werden.

**Anlage -2-
zur Dienstanweisung Nr. 22/96**

Zu Punkt 2.2.2.

Auszüge aus dem Bbg DSG

**§ 5 Bbg DSG
Rechte des Betroffenen**

(1) Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft und Benachrichtigung über die zu seiner Person gespeicherten Daten sowie Einsicht in Akten (§ 18).
2. Berichtigung, Löschung oder Sperrung der zu seiner Person gespeicherten Daten (§ 19).
3. Schadensersatz (§ 20).
4. Anrufung des Landesbeauftragten für den Datenschutz (§ 21 Abs. 1).

Diese Rechte können auch durch die Einwilligung des Betroffenen nicht ausgeschlossen oder beschränkt werden. Sie sind gegenüber der jeweiligen datenverarbeitenden Stelle geltend zu machen.

- (2) Sind die Daten des Betroffenen in einer Datei gespeichert, bei der mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage, die datenverarbeitende Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die datenverarbeitende Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die datenverarbeitende Stelle zu unterrichten. Die in § 19 Abs. 3 des Bundesdatenschutzgesetzes genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Landesbeauftragten für den Datenschutz über die Weiterleitung und die datenverarbeitende Stelle unterrichten. In diesem Fall richtet sich das weitere Vorgehen nach § 18 Abs. 8.

§ 18 Bbg DSG

Auskunft und Benachrichtigung sowie Einsicht in Akten

- (1) Dem Betroffenen ist von der datenverarbeitenden Stelle auf Antrag Auskunft zu erteilen über
 1. die zu seiner Person gespeicherten Daten,
 2. den Zweck und die Rechtsgrundlage der Speicherung sowie
 3. die Herkunft der Daten, den Zweck der Übermittlung und die Empfänger von regelmäßigen Übermittlungen und die Teilnehmer eines automatisierten Abrufverfahrens, auch soweit diese Angaben nicht zu seiner Person gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Sind die Daten in einer Datei gespeichert, so umfasst die Auskunft auch die Empfänger von Übermittlungen innerhalb der letzten zwei Jahre. In Akten sind Übermittlungen zu dokumentieren.
- (2) Werden personenbezogene Daten in einer automatisierten Datei gespeichert, so ist der Betroffene von dieser Tatsache schriftlich zu benachrichtigen. Die Benachrichtigung kann zusammen mit der Erhebung erfolgen.
- (3) Die Absätze 1 und 2 gelten nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.
- (4) Die datenverarbeitende Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen; sind die Daten in Akten gespeichert, ist dem Betroffenen auf Verlangen Einsicht zu gewähren. Die Akteneinsicht ist auf die Teile der Akten beschränkt, die personenbezogene Daten des Betroffenen enthalten, soweit sich aus einem Verwaltungsverfahrensgesetz nichts anderes ergibt. Auskunft aus Akten oder Akteneinsicht sind zu gewähren, soweit der Betroffene Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen. Auskunftserteilung und Akteneinsicht sind gebührenfrei; Erstattung von Auslagen kann verlangt werden.
- (5) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht sowie zur Benachrichtigung entfällt, soweit die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen eines Dritten geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.
- (6) Einer Begründung für die Auskunftsverweigerung bedarf es nur dann nicht, wenn durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen.

- (7) Bezieht sich die Auskunftserteilung oder die Akteneinsicht auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, sowie von den in § 19 Abs. 3 des Bundesdatenschutzgesetzes genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Für die Versagung der Zustimmung gelten, soweit dieses Gesetz auf die genannten Behörden Anwendung findet, die Absätze 5 und 6 entsprechend.
- (8) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Landesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der datenverarbeitenden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

§ 19

Berichtigung, Löschung und Sperrung

- (1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten in nicht-automatisierten Dateien oder in Akten zu berichtigen, so ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind.
- (2) Personenbezogene Daten sind zu löschen, wenn
- a) ihre Speicherung unzulässig ist oder
 - b) ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Satz 1 Buchstabe b nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, dass der Betroffene die Löschung verlangt und die weitere Speicherung ihn in unangemessener Weise beeinträchtigen würde. Soweit hiernach eine Löschung nicht in Betracht kommt, sind die personenbezogenen Daten auf Antrag des Betroffenen zu sperren.

(3) An die Stelle einer Löschung tritt eine Sperrung der personenbezogenen Daten, wenn

- a) ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
- b) der Betroffene an Stelle der Löschung nach Absatz 2 Satz 1 Buchstabe a die Sperrung verlangt,
- c) die weitere Speicherung im Interesse des Betroffenen geboten ist,
- d) sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind oder
- e) die Voraussetzungen des Absatzes 2 Satz 1 Buchstabe b vorliegen und die Daten aber auf Grund gesetzlicher Aufbewahrungsfristen nicht gelöscht werden dürfen.

In den Fällen nach Satz 1 Buchstabe c sind die Gründe aufzuzeichnen. Bei automatisierten Dateien ist die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen; im übrigen ist ein entsprechender Vermerk anzubringen. Gesperrte Daten dürfen über die Speicherung hinaus nicht mehr weiterverarbeitet werden, es sei denn, dass dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der datenverarbeitenden Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene eingewilligt hat.

(4) Abgesehen von den Fällen des Absatzes 2 Satz 1 Buchstabe a ist von einer Löschung abzusehen, soweit die gespeicherten Daten auf Grund von Rechtsvorschriften einem Archiv zur Übernahme anzubieten oder von einem Archiv zu übernehmen sind.

(5) Über die Berichtigung unrichtiger Daten, die Sperrung bestrittener Daten und die Löschung oder Sperrung unzulässig gespeicherter Daten sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt worden sind. Die Unterrichtung kann unterbleiben, wenn sie einen erheblichen Aufwand erfordern würde und nachteilige Folgen für den Betroffenen nicht zu befürchten sind.

§ 20 Schadensersatz

(1) Wird dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt, so ist ihm der Träger der datenverarbeitenden Stelle unabhängig von einem Verschulden zum Schadensersatz verpflichtet. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 500 000 Deutsche Mark.

- (2) Auf eine schuldhafte Mitverursachung des Schadens durch den Betroffenen und die Verjährung des Entschädigungsanspruches sind die §§ 254, 839 Abs. 3 und § 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.
- (3) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.
- (4) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

§ 21 Bbg DSG **Anrufungsrecht des Betroffenen**

- (1) Jedermann hat das Recht, sich unmittelbar an den Landesbeauftragten für den Datenschutz zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine der Kontrolle des Landesbeauftragten unterliegende Stelle in seinen Rechten verletzt zu sein; dies gilt auch für Bedienstete der öffentlichen Stellen, ohne dass der Dienstweg einzuhalten ist.
- (2) Niemand darf deswegen benachteiligt oder gemäßregelt werden, weil er sich an den Landesbeauftragten für den Datenschutz wendet.

**Anlage -3-
zur Dienstanweisung Nr. 22/96**

Zu Punkt 2.2.3.

Muster der Verpflichtung

Verpflichtung auf das Datengeheimnis
(gemäß § 6 Brandenburgisches Datenschutzgesetz - Bbg DSG)

Hiermit erkläre ich, _____,
Stelle _____, dass ich heute über die einschlägigen
Vorschriften des Brandenburgischen Datenschutzgesetzes in Kenntnis gesetzt, über die
sich daraus ergebenen besonderen Anforderungen an die Datensicherheit und den
Datenschutz bei der Ausübung meiner Tätigkeit vertraut gemacht und auf das Datenge-
heimnis verpflichtet wurde.

Ich wurde insbesondere darüber belehrt, dass es mir untersagt ist, geschützte personen-
bezogene Daten zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabener-
füllung gehörenden Zweck zu verarbeiten oder zu nutzen.

Diese Pflicht besteht auch nach Beendigung meiner Tätigkeit fort.

Mir ist bekannt, dass Verstöße gegen das Datengeheimnis sowohl arbeits- als auch
strafrechtlich verfolgt werden können. Sie können auch Anlass zu einer außerordent-
lichen Kündigung sein.

Meine sich aus Arbeitsvertrag und -ordnung ergebende Geheimhaltungsverpflichtung wird
durch diese Verpflichtung nicht berührt.

Einen Abdruck dieser Verpflichtungserklärung und ein Merkblatt zum Datenschutz habe
ich erhalten.

(Ort, Datum)

(Unterschrift Verpflichteter)

(Unterschrift Verpflichtender)

Merkblatt zum Datenschutz

Sehr geehrte/r Frau/Herr,

es ist sicher nicht in Ihrem Sinne, wenn Daten über ihre Person und über ihre persönlichen Verhältnisse Unbefugten zur Kenntnis gelangen würden. Davor schützen Sie das Bbg DSG und andere bereichsspezifische Datenschutzregelungen.

Aber auch Sie sind im Rahmen Ihrer beruflichen Tätigkeit dazu verpflichtet, die personenbezogenen Daten anderer vertraulich und weisungsgerecht zu behandeln.

Sie sind dafür verantwortlich, dass die Ihnen anvertrauten personenbezogenen Daten nur im Rahmen Ihrer Aufgabenstellung verarbeitet (gespeichert, verändert, übermittelt, gesperrt, gelöscht) oder genutzt werden. Der Missbrauch und jede unbefugte Weitergabe dieser Daten sind unzulässig und strafbar.

Insbesondere sind Sie persönlich dafür verantwortlich, dass

- die Ihnen anvertrauten Daten und Datenträger, wenn Sie nicht unmittelbar daran arbeiten, unter Verschluss gehalten werden,
- Ihr Datenverarbeitungs-Gerät (DV-Gerät), Ihre Anwendungen und Ihr Passwort keinem Unbefugten zugänglich gemacht werden,
- nicht mehr benötigte personenbezogene Datenträger datenschutzgerecht vernichtet werden, damit eine mißbräuchliche Weiterverwendung nicht mehr möglich ist.

Es ist Ihnen untersagt, behördeneigene DV-Geräte privat zu nutzen oder private Computer, Software und Datenträger in die Kreisverwaltung mitzubringen, da sonst eine wirksame Kontrolle des Datenschutzes innerhalb unserer Behörde erheblich erschwert wird.

Sie wurden auf das Datengeheimnis verpflichtet, das auch nach Beendigung Ihrer Tätigkeit fortbesteht.

Bei Fragen zum Datenschutz oder in Zweifelsfragen wenden Sie sich bitte an Ihre Vorgesetzten oder - in besonderen Fällen - an den Datenschutzbeauftragten Herrn Hoffmann Tel. 03371/688560, der Kreisverwaltung Teltow-Fläming.

**Anlage -4-
zur Dienstanweisung Nr. 22/96**

Zu Punkt 2.2.4.

Auszüge aus dem Bbg DSG

**§ 7 Bbg DSG
Sicherstellung des Datenschutzes**

- (1) Die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen haben jeweils für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Sie haben insbesondere dafür zu sorgen, dass die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, gewährleistet ist.
- (2) Vor dem Erlass von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, ist der Landesbeauftragte für den Datenschutz zu hören.
- (3) Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf hinsichtlich der in der Dateibeschreibung festzulegenden Angaben (§ 8 Abs. 1) der schriftlichen Freigabe. In der Landesverwaltung ist die Freigabe durch diejenige oberste Landesbehörde zu erklären, die für die dem automatisierten Verfahren zugrunde liegende Rechtsmaterie zuständig ist. Im übrigen erfolgt die Freigabe durch die datenverarbeitende Stelle. Entsprechendes gilt für wesentliche Änderungen des Verfahrens.

§ 8 Bbg DSG **Dateibeschreibung**

- (1) Die datenverarbeitende Stelle ist verpflichtet, in einer Dateibeschreibung schriftlich festzulegen:
1. die Bezeichnung der Datei und ihre Zweckbestimmung,
 2. die Art der gespeicherten Daten sowie die Rechtsgrundlage ihrer Vereinbarung,
 3. den Kreis der Betroffenen,
 4. die Art regelmäßig zu übermittelnder Daten, deren Empfänger sowie die Herkunft regelmäßig empfangener Daten,
 5. Fristen für die Sperrung und Löschung der Daten,
 6. die technischen und organisatorischen Maßnahmen gemäß § 10,
 7. bei automatisierten Verfahren die Betriebsart des Verfahrens, die Art der Geräte, die Stellen, bei denen sie aufgestellt sind, sowie das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung.
- (2) Absatz 1 findet keine Anwendung auf nicht-automatisierte Dateien, aus denen keine Daten an Dritte übermittelt werden, sowie auf Dateien, die bei automatisierter Verarbeitung ausschließlich aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden.
- (3) Die Landesregierung wird ermächtigt, nach Anhörung des Landesbeauftragten für den Datenschutz den näheren Inhalt der Dateibeschreibung nach Absatz 1 durch Rechtsverordnung zu bestimmen.
- (4) Die datenverarbeitende oder die in ihrem Auftrag tätige Stelle ist verpflichtet, in einem Verzeichnis der Geräte, mit denen personenbezogene Daten automatisiert verarbeitet werden, festzulegen:
1. den Typ und die Art der Geräte,
 2. den Hersteller,
 3. Anzahl der Geräte,
 4. das verwendete Betriebssystem und
 5. die Möglichkeiten zur Datenfernverarbeitung und Datenübertragung.

Das Verzeichnis ist laufend auf dem neuesten Stand zu halten. Weitere in das Verzeichnis aufzunehmende Angaben über die Beschaffenheit der Geräte und deren Verwendung bestimmt das Ministerium des Innern durch Rechtsverordnung nach Anhörung des Landesbeauftragten für den Datenschutz.

§ 9 Bbg DSG

Automatisiertes Abrufverfahren und regelmäßige Datenübermittlung

- (1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufes bleiben unberührt.
- (2) Die Minister werden ermächtigt, für die Behörden und Einrichtungen ihres Geschäftsbereiches sowie für die der Rechtsaufsicht des Landes unterliegenden sonstigen öffentlichen Stellen die Einrichtung automatisierter Abrufverfahren durch Rechtsverordnung zuzulassen. Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. Die Datenempfänger, die Datenart und der Zweck des Abrufes sind festzulegen. Der Landesbeauftragte für den Datenschutz ist zu unterrichten.
- (3) Die am Abrufverfahren beteiligten Stellen haben die nach § 10 erforderlichen Maßnahmen zu treffen.
- (4) Für die Einrichtung automatisierter Abrufverfahren innerhalb einer öffentlichen Stelle gelten nur Absatz 2 Satz 2 und 3 sowie Absatz 3 entsprechend.
- (5) Personenbezogene Daten dürfen für Stellen außerhalb des öffentlichen Bereiches nicht zum automatisierten Abruf bereitgehalten werden; dies gilt nicht für den Betroffenen.
- (6) Die Absätze 1 bis 5 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offenstehen oder deren Veröffentlichung zulässig wäre.
- (7) Absatz 1 Satz 1 und Absatz 2 Satz 1 und 4 sowie Absatz 5 finden keine Anwendung, soweit die zur Übermittlung vorgesehenen Daten mit schriftlicher Einwilligung der Betroffenen zum Zwecke der Übermittlung im automatisierten Abrufverfahren gespeichert sind, § 4 Abs. 2 Satz 2 und 3 gilt entsprechend.
- (8) Die Absätze 1 bis 7 sind auf die Zulassung regelmäßiger Datenübermittlungen entsprechend anzuwenden.

§ 10 BbgDSG

Technische und organisatorische Maßnahmen

- (1) Öffentliche Stellen, die selbst oder im Auftrag einer anderen öffentlichen Stelle personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
- (2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind,
 1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
 2. zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),
 3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
 4. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),
 5. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
 6. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit an wen durch Einrichtungen zur Datenübertragung übermittelt worden sind (Übermittlungskontrolle),
 7. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
 8. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

9. zu gewährleisten, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern diese nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),
 10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).
-
- (3) Werden personenbezogene Daten in nicht-automatisierten Dateien oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.
 - (4) Soweit Vorentwürfe und Notizen nicht Bestandteil eines Vorganges werden und personenbezogene Daten enthalten, ist eine ordnungsgemäße Vernichtung zu gewährleisten.

§ 11 Bbg DSG

Verarbeitung personenbezogener Daten im Auftrag

- (1) Werden personenbezogene Daten im Auftrag einer öffentlichen Stelle verarbeitet, so bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung seiner Eignung für die Gewährleistung der nach § 10 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei erforderlichenfalls ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Soweit der Auftragnehmer keine öffentliche Stelle im Sinne des § 2 Abs. 1 Satz 1 ist, bedarf die Auftragserteilung der Zustimmung; bei öffentlichen Stellen des Landes erteilt die Zustimmung die zuständige oberste Landesbehörde, bei Gemeinden und Gemeindeverbänden der Minister des Innern.
- (2) Soweit das Landesamt für Datenverarbeitung und Statistik (Landesdatenverarbeitungszentrale), die gemeinsamen Gebietsrechenzentren, die Fachrechenzentren, die Hochschulrechenzentren und die kommunalen Datenverarbeitungseinrichtungen personenbezogene Daten im Auftrag öffentlicher Stellen verarbeiten, gelten für sie außer §§ 6 und 10 auch §§ 21, 23, 25 und 26 dieses Gesetzes unmittelbar.

- (3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Landesbeauftragten für den Datenschutz unterwirft. Bei einer Auftragsdurchführung außerhalb des Geltungsbereiches dieses Gesetzes ist die für den Ort der Auftragsdurchführung zuständige Datenschutzkontrollbehörde zu unterrichten. Der Auftraggeber hat den Datenschutzbeauftragten und die im Land Brandenburg nach § 38 des Bundesdatenschutzgesetzes zuständige Aufsichtsbehörde über die Beauftragung zu unterrichten.
- (4) Sofern Unterauftragsverhältnisse vorgesehen sind oder zugelassen werden sollen, ist vertraglich sicherzustellen, dass die datenschutzrechtlichen Pflichten in dem gleichen Umfang eingehalten werden, wie sie im Auftragsverhältnis mit der öffentlichen Stelle festgelegt sind; Absatz 3 gilt entsprechend.

§ 11 a **Wartung und Fernwartung**

- (1) Bei der Wartung von Datenverarbeitungssystemen hat die datenverarbeitende Stelle sicherzustellen, dass technische und organisatorische Maßnahmen getroffen werden, die eine unbefugte Offenbarung personenbezogener Daten ausschließen.
- (2) Sofern dies nicht sichergestellt werden kann, darf die Wartung oder Fernwartung von Datenverarbeitungssystemen durch andere Stellen nur aufgrund schriftlicher Vereinbarungen erfolgen. In der Vereinbarung sind die im Rahmen der Wartung und Fernwartung notwendigen technischen und organisatorischen Maßnahmen (§ 10) festzulegen. Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses schriftlich zu verpflichten.

**Anlage -5-
zur Dienstanweisung Nr. 22/96**

Zu Punkt 2.2.4.5.

Einbeziehung und Pflichten des Personalrates:

Auszüge aus dem Pers VG

**§ 60 (5) Pers VG
Unterrichtung des Personalrates**

Die Dienststelle soll den Personalrat in geeigneten Fällen in die Vorbereitung beteiligungspflichtiger Maßnahmen einbeziehen, insbesondere kann einem Mitglied die Teilnahme in Planungsgruppen oder Ausschüssen, die beteiligungspflichtige Maßnahmen der Dienststelle vorbereiten sollen, gestattet werden.

**§ 65 Pers VG
Mitbestimmung bei organisatorischen Angelegenheiten**

Der Personalrat hat in folgenden organisatorischen Angelegenheiten mitzubestimmen:

1. Einführung, Anwendung, wesentliche Änderung oder wesentliche Erweiterung von automatisierter Verarbeitung personenbezogener Daten der Beschäftigten, außerhalb von Besoldungs-, Vergütungs-, Lohn- und Versorgungsleistungen sowie von Beihilfen,
2. Einführung, Anwendung, Änderung oder wesentliche Erweiterung von technischen Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen,
3. Einführung wesentliche Änderung oder wesentliche Ausweitung neuer Arbeitsmethoden, insbesondere Maßnahmen der technischen Rationalisierung,
4. Auslagerung von Arbeitsplätzen zwecks Heimarbeit an technischen Geräten,
5. Allgemeine Maßnahmen zur Hebung der Arbeitsleistung oder zur Erleichterung des Arbeitsablaufs sowie Maßnahmen zur Änderung der Arbeitsorganisation, soweit sie nicht von den Nummern 3 oder 4 erfasst sind.

**§ 66 Nr. 13 Pers VG
Mitbestimmung bei sonstigen innerdienstlichen Angelegenheiten**

Der Personalrat hat in folgenden innerdienstlichen Angelegenheiten mitzubestimmen:

13. Inhalt von Personalfragebogen, mit Ausnahme von Fragebogen im Rahmen der Rechnungsprüfung und von Organisationsunterlagen

§ 68 (3) Nr. 1 PersVG
Fälle der Mitwirkung

(3) Der Personalrat wirkt bei folgenden sonstigen innerdienstlichen Angelegenheiten mit:

1. Aufstellung von Vorschriften und Verwaltungsanordnungen, durch die der innerdienstliche Betrieb in der Dienststelle geregelt wird, soweit persönliche oder soziale Belange der Beschäftigten berührt werden.

§ 10 PersVG
Schweigepflicht

- (1) Personen, die Aufgaben oder Befugnisse nach diesem Gesetz wahrnehmen oder wahrgenommen haben, haben über die ihnen dabei bekanntgewordenen Angelegenheiten und Tatsachen Stillschweigen zu bewahren.
- (2) Die Schweigepflicht gilt nicht für Mitglieder des Personalrates untereinander sowie gegenüber der Jugend- und Auszubildendenvertretung, den Ersatzmitgliedern sowie Vertrauensleuten nach diesem Gesetz; gleiches gilt gegenüber den zuständigen Schwerbehindertenvertretungen, gegenüber der Einigungsstelle, gegenüber der Stufenvertretung sowie gegenüber den Vertrauensleuten der Zivildienstleistenden. Dürfen Informationen nur mit Zustimmung der betroffenen Beschäftigten der Personalvertretung oder einzelnen Mitgliedern zugänglich gemacht werden, dürfen Sie nur mit deren Zustimmung an die in Satz 1 genannten Stellen weitergegeben werden.
- (3) Die Schweigepflicht gilt entsprechend für Personen, die das Protokoll führen und für Ersatzmitglieder. Sie gilt ferner für die Dienststellenleitung und alle anderen Personen, die an der Sitzung teilnehmen oder mit denen der Personalrat nach diesem Gesetz zusammenarbeitet.
- (4) Die Schweigepflicht besteht nicht für Angelegenheiten oder Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

§ 94 (3) PersVG
Datenschutz

- (3) Personenbezogene Daten in Akten oder Datenträgern sind zu löschen bzw. zu vernichten, sobald sie zur Aufgabenerfüllung nicht mehr erforderlich sind und besondere gesetzliche Regelungen nichts anderes bestimmen.

**Anlage -6-
zur Dienstanweisung Nr. 22/96**

Materialgröße nach der Entsorgung (Vernichtung) gem. DIN 32757:

Schutz- stufe nach	Sicher- heitsstufe	Vertraulichkeitsgrad Mikrofilm, nach DIN 32 757	Form des Abfallgutes Chipkarte	Papier	
Schutz- stufen- Länge konzept	nach DIN max. Toleranzbereich 32 757 Fläche			max. Breite	max.
(siehe Punkt 3.1)	Anteil der Stich- probe (mm2) (%)	Max. der Teilchen fläche (mm2)		(mm)	(mm)
	1 unendlich	allgem. Schriftgut - ohne bes. Vertrau- lichkeit 3800	Streifen	12	
	- 2000 10		Partikel	-	
A	2 unendlich	internes Schriftgut - -	Streifen	6	
-	800 10	2000	Partikel	-	
B	3	vertraulich	Streifen	2	
-	594 -	- -			
			Partikel	4	
80	320 10	800 1			
C	4	geheim	Partikel	2	
15	30 10	90 0,5			
D	5	streng	Partikel	0,8	
13	10 10	30 0,2			