Dienstanweisung Datenschutz und Datensicherheit
für den Landkreis Mansfeld-Südharz

Inhalt:

Anlage 5
Prüfansätze Verfahrensfreigabe

Anlage 6
Einsatz und Betrieb der Informations- und Kommunikationstechnik für das Haushalts- und Kassenwesen

Anlage 7
Regelungen für den Einsatz von E-Mail

Teil I

1. Grundlagen dieser Dienstanweisung sind

- Verfassung des Landes Sachsen-Anhalt vom 16.07.1992 (GVBl. LSA 1992, S. 600), geändert durch Gesetz vom 27.01.2005 (GVBl. LSA S. 44);
- bereichsspezifische Rechtsgrundlagen (z.B. Sozialgesetzbuch - SGB);
- DSG-LSA in der Fassung der Bekanntmachung vom 18.02.2002 (GVBl. LSA S. 54), zuletzt geändert durch Artikel 15 des Ersten Rechts- und Verwaltungsvereinfachungsgesetzes vom 18.11.2005 (GVBl. LSA S. 698, 701);
- BDSG in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. August 2006 (BGBl. I S. 1970).

2. Allgemeines

Beim Umgang mit personenbezogenen Daten, insbesondere beim Einsatz moderner Informations- und Kommunikationstechnologien sind Vorkehrungen und Regelungen zur Gewährleistung des Datenschutzes und der Datensicherung/Datensicherheit zu treffen. Dabei sind rechtliche, organisatorische, technische und bauliche Aspekte zu beachten.

3. Geltungsbereich

Diese Dienstanweisung gilt für alle Organisationseinheiten des Landkreises Mansfeld-Südharz ungeachtet ihrer Rechtsform, die personenbezogene Daten verarbeiten oder durch andere verarbeiten lassen und keinen eigenen Datenschutzbeauftragten eingesetzt sowie eigene Festlegungen für die Durchführung des Datenschutzes und der Datensicherheit getroffen haben.

4. Umfang des Datenschutzes

Zweck des Datenschutzes ist es, den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
Aus diesem Grund ist das Erheben, Verarbeiten (Speichern, Verändern, Übermitteln, Sperren und Löschen) sowie das Nutzen personenbezogener Daten nur mit Einwilligung des Betroffenen oder auf gesetzlicher Grundlage zulässig.
Dabei ist nicht entscheidend, wo und auf welche Weise dies geschieht, z.B. als Akte, als nicht automatisierte Datei (Kartei) oder als automatische Datei im Großrechner, Abteilungsrechner, Mehrplatzsystem, Einzelplatzrechner (Recht auf informationelle Selbstbestimmung).
Das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) gilt sowohl für die herkömmliche Informationsverarbeitung in Akten wie für die Anwendung moderner Informations- und Kommunikationstechniken.

Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind die verfassungsrechtlichen Grundsätze der Verhältnismäßigkeit sowie der Zweckbindung und informationellen Gewaltenteilung auch innerhalb des Landkreises zu beachten. Durch geeignete organisatorische und technische Vorkehrungen ist zu gewährleisten, dass

a) sich das Erheben, Verarbeiten oder nutzen personenbezogener Daten nach für den Betroffenen erkennbaren Regeln vollzieht und
b) Verstöße gegen das Recht auf informationelle Selbstbestimmung verhindert werden.

Die im Rahmen der organisatorischen und technischen Vorkehrungen gespeicherten Daten der Beschäftigten dürfen nicht zu Zwecken der Verhaltens- und Leistungskontrolle genutzt werden (§ 28 Abs. 5 DSG-LSA).

5. Rechts- und Verwaltungsvorschriften

Die Zulässigkeit und der Umfang der Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Einzelfall richten sich nach den einschlägigen bereichsspezifischen gesetzlichen Bestimmungen oder, wenn solche nicht vorhanden sind, nach dem DSG-LSA.
Auf die paragraphenweise gegliederten Verwaltungsvorschriften Gem. RdErl. des MI, der StK und der übrigen Min. vom 31.8.2002-41.21B-05519/1 - (MBl.LSA S. 1091), geändert durch Gem. RdErl. des MI, der StK und der übrigen Min. vom 13.7.2007-41.21A-05519/2 (MBl. LSA S. 629) und vom 12.11.2007 - 41.21A-05519/2 (MBl. LSA S. 834) zu diesem Gesetz wird hingewiesen.

Speichernde Stelle im Sinne des DSG-LSA ist der Landkreis Mansfeld-Südharz als Gesamtbehörde. Die Weitergabe personenbezogener Daten innerhalb des Landkreises Mansfeld-Südharz ist grundsätzlich keine Übermittlung. Gleichwohl ist die interne Weitergabe grundsätzlich nur zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung erforderlich ist und die Daten für den Zweck weitergegeben werden, für den sie erhoben, oder gespeichert worden sind.

Zur Zweckbindung wird auf die Verwaltungsvorschrift zu § 10 DSG-LSA verwiesen. Eine Zweckänderung ist nur unter den in § 10 Abs. 2 DSG-LSA genannten Voraussetzungen zulässig.

Für Sozialleistungsträger ist § 67c Abs. 1 SGB X entsprechend anzuwenden, der die Zweckbindungsgrundsätze für die in § 35 SGB I genannten Stellen darstellt.
Bei der Zweckbindung nach § 78 SGB X handelt es sich um Personen oder Dritte, die nicht zum Empfängerkreis der in § 35 SGB I genannten Stellen gehören, so dass befugt übermittelte Sozialdaten nach den §§ 68 bis 77 SGB X den Schutz der Sozialdaten durch Übermittlung an Dritte nicht verschlechtert.

Das Amt für Gesundheit hat eine Vielzahl unterschiedlicher Aufgaben zu erfüllen, so dass eine Vielzahl äußerst sensibler Daten anfällt. Diese sind nicht nur durch die Vorschriften des Gesetzes über den Öffentlichen Gesundheitsdienst und die Berufsausübung im Gesundheitswesen im Land Sachsen-Anhalt (Gesundheitsdienstgesetz - GDG LSA - GVBl. LSA 1997, S. 1023) besonders zu schützen, sie unterliegen in der Regel auch dem Patientengeheimnis.
Soweit das GDG LSA nichts anderes bestimmt, findet das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) Anwendung.

6. Zuständigkeiten

6.1 Allgemeines

Datenschutz ist in erster Linie Aufgabe der Organisationseinheit, die im Rahmen ihrer Zuständigkeit personenbezogene Daten erhebt, verarbeitet oder nutzt bzw. verarbeiten oder nutzen lässt.

Die Mitwirkung anderer Organisationseinheiten bei der Verarbeitung personenbezogener Daten in automatisierten Verfahren berührt die Verantwortlichkeit der Organisationseinheiten für den Schutz "ihrer" Daten grundsätzlich nicht.

6.2 Aufgaben der Organisationseinheiten

- Prüfen der anwendbaren Rechtsvorschriften,

- Prüfen der Zulässigkeit der Erhebung, Speicherung, Veränderung, Nutzung, Sperrung und Löschung,

- Prüfen der Zulässigkeit der Datenübermittlung innerhalb des öffentlichen Bereiches und an Stellen außerhalb des öffentlichen Bereiches,

- Auskünfte an Betroffene (§ 15 DSG-LSA),

- Auskünfte an Betroffene durch Sozialleistungsträger (§ 83 SGB X),

- Auskünfte an Betroffene durch das Jugendamt (§ 67 SGB VIII i.V.m. § 83 SGB X).

Auskünfte an den Betroffenen, welche Daten über ihn gespeichert sind, erteilen grundsätzlich die Organisationseinheiten, sofern sich der Antrag lediglich auf deren Aufgabenbereich bezieht.

Allgemein gehaltene Auskunftswünsche (z.B. Betroffener will über **alle** Daten informiert werden, die zu seiner Person gespeichert sind) sind an die Zentrale Verwaltung abzugeben. Das Rechtsamt sollte eingeschaltet werden, wenn die Auskunftserteilung nach § 15 Abs. 4 DSG-LSA sowie durch die Sozialleistungsträger nach § 83 Abs. 4 SGB X unterbleibt.

Für Auskünfte sind Kosten (Gebühren und Auslagen) nicht zu erheben.

Die Auskunft über Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen nicht gelöscht werden dürfen, wird nur auf besonderen von dem Betroffenen zu stellenden Antrag erteilt.
Wenn mit dieser Auskunfserteilung ein besonderer Verwaltungsaufwand verbunden ist, muss der Betroffene in Kentnis gesetzt werden, dass gemäß § 15 Abs. 1a DSG-LSA diese der Kostenpflicht unterliegt. Nach Auskunftserteilung sind sie dem Antragsteller in analoger Anwendung der Satzung des Landkreises Mansfeld-Südharz über die Erhebung von Verwaltungskosten im eigenen Wirkungskreis in Rechnung zu stellen.
Für den Bereich der Sozialleistungsträger kann § 15 Abs. 1a DSG-LSA i.V.m. § 15 Abs. 7 Satz 2 DSG-LSA nicht gelten, da eine vergleichbare Reglung in § 83 SGB X nicht aufgenommen wurde.

Sofern die Voraussetzungen des § 16 DSG-LSA, bei den Sozialleistungsträgern des § 84 SGB X vorliegen, hat der Betroffene Anspruch auf Berichtigung, Sperrung und Löschung seiner personenbezogenen Daten.

- Datengeheimnis (§ 5 DSG-LSA);
  Die mit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beauftragten Mitarbeiter haben neben den ohnehin für sie geltenden allgemeinen Verschwiegenheitspflichten (z.B. § 203 StGB, § 3 TVöD, § 61 BG LSA) das Datengeheimnis zu wahren.

  Sie sind durch die Organisationseinheit über das Datengeheimnis schriftlich zu belehren (**siehe Anlage 1**), aber nicht förmlich zu verpflichten. Auf Anforderung der Organisationseinheit kann diese Aufgabe auch dem Datenschutzbeauftragten übertragen werden.

  Auftragnehmer i.S. des § 8 Abs. 5 DSG-LSA haben ihre Mitarbeiter nach § 5 des Bundesdatenschutzgesetzes (schriftlich) auf das Datengeheimnis zu verpflichten.

- Personenbezogene Arbeitnehmerdaten (§ 28 DSG-LSA);
  Für die Erhebung, Verarbeitung und Nutzung von Personalakten- und Bewerberdaten gelten die Regelungen des § 28 DSG-LSA und 90 ff BG LSA. Das DSG-LSA findet auf Sachaktendaten

Anwendung.

Beim Einsatz automatisierter Verfahren sind darüber hinaus die Mitbestimmungsrechte der Personalvertretung zu beachten (z.B. § 69 Nr. 1 und 2 Landespersonalvertretungsgesetz LSA), soweit die Datenverarbeitung der Vorbereitung personalrechtlicher Entscheidungen usw. dient oder geeignet ist, das Verhalten oder die Leistung der Angehörigen der Dienststelle zu überwachen.

Die Erfassung von personenbezogenen Daten über die Benutzung von Telekommunikationsanlagen erfolgt entsprechend den Richtlinien über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen vom 09.04.1999 (MBl. LSA 1999 S. 565).

- Vordruckwesen

Die Organisationseinheiten sind dafür verantwortlich, dass sie (per Vordruck) von dem Betroffenen nur die Daten erheben, die sie konkret zur rechtmäßigen Aufgabenerfüllung im Einzelfall benötigen. Bei der Gestaltung von Vordrucken sind die bereichsspezifischen Rechtsgrundlagen zu beachten (z.B. § 67a SGB X). Sind diese nicht vorhanden, sind §§ 4 und 9 DSG-LSA mit den entsprechenden Anmerkungen der VV-DSG-LSA zu beachten. Im Sozialleistungsbereich sind außerdem die §§ 13 bis 17 SGB I zu beachten.

- Behandlung der Datenträger

Die Ämter sind dafür verantwortlich, dass Datenträger, z.B. Papier, Einmal-Farbbänder, Magnetplatten, Magnetbänder, Disketten, Wechselfestplatten, optoelektronische Datenträger usw., mit personenbezogenen Daten unbefugten Personen nicht zugänglich sind.
Vor der Vernichtung von Datenträgern wird auf die Übergabe nach § 11 Landesarchivgesetz (ArchG.LSA) hingewiesen.
Datenträger sind, wenn sie vernichtet werden sollen und nicht unmittelbar einem Aktenschredder zugeführt werden, bis zur Vernichtung in geeigneten verschließbaren Behältnissen aufzubewahren. Bei der Vernichtung von Datenträgern und veralteten Unterlagen sind die in der **Anlage 2** getroffenen Regelungen zu beachten.

6.3 Aufgaben der Zentralen Verwaltung - Sachgebiet EDV

- Auswahl angemessener technischer und organisatorischer Maßnahmen zur Datensicherheit in Zusammenarbeit mit der verantwortlichen Stelle (§ 6 DSG-LSA),

- Überwachung der ordnungsgemäßen Anwendung der Programme bei zentraler und dezentraler Datenverarbeitung, einschließlich deren Pflege und Dokumentation,

- Führen des Verzeichnisses der eingesetzten Datenverarbeitungsanlagen,

- federführend für einen reibungslosen technischen Arbeitsablauf, einschließlich des Bereiches der Datensicherung;
Die Störungsbeseitigung unter Nutzung des Zugriffsrechtes des Systemverwalters und bei Beendigung des Zugriffes ist dem Betreiber der Anlage anzuzeigen.

- Vorabkontrolle vor Freigabe bzw. wesentliche Änderung der in § 14 Abs. 2 DSG-LSA genannten automatisierten Verfahren in Bezug auf technisch-organisatorische Maßnahmen,

- Freigabe des Verfahrens nach dem Muster der **Anlage 3,**

- Bearbeiten pauschal abgefaßter (amtsübergreifender) Auskunftsersuchen,

- Bearbeiten allgemeiner ämterübergreifende Angelegenheiten des Datenschutzes.

Die Systembeauftragten des Sachgebietes EDV sind befugt, den Benutzern der Anlage im Einvernehmen mit dem jeweiligen Leiter der Organisationseinheit nötigenfalls Weisungen zu erteilen.

6.4 Aufgaben des Beauftragten für den Datenschutz

- Beratung der Verwaltungsleitung, der Mitarbeiter und des Personalrates in datenschutzrelevanten Fragen
- Durchführung von Kontrollen

Zu diesem Zweck hat er Zutritt zu allen Diensträumen und kann alle dienstlichen Unterlagen einsehen, die personenbezogene Daten enthalten oder den Umgang mit diesen betreffen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. (§ 14a Abs. 3 Satz 1 und 3 DSG-LSA). Gem. § 14a Abs. 3 Satz 2 DSG-LSA gilt dies nicht, wenn Berufs- oder besondere Amtsgeheimnisse entgegenstehen.

- Führung des Verfahrensverzeichnisses gem. § 14a Abs. 4 Satz 1 DSG-LSA **(siehe Anlage 4)**

- Sammlung der Nachweise zur datenschutzrechtlichen Vorabkontrolle (§ 14a Abs. 4 Satz 2 Ziffer 2 DSG-LSA) von automatisierten Verfahren

- Unterrichtung des Landesbeauftragten für Datenschutz LSA (LfD LSA) über die Errichtung automatisierter Abrufverfahren (§ 7 Abs. 3 DSG-LSA)

- Unterrichtung des LfD LSA über die Auftragsdatenverarbeitung nicht-öffentlicher Stellen (§ 8 Abs. 6 DSG LSA)

- Kontrolle der Einhaltung des Datenschutzes bei Auftragnehmern bei der Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 8 DSG-LSA)

- Erarbeitung oder Mitwirkung bei der Erstellung von Richtlinien, Rundschreiben, Dienstvereinbarungen und weiteren allgemeinen Verlautbarungen, die den Umgang mit personenbezogenen Daten betreffen

- Mitwirkung bei der Erarbeitung und Anwendung datenschutzgerechter Verwaltungsunterlagen (Vordrucke und Merkblätter)

- Mitwirkung bei Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsverlangen nach §§ 15 und 16 DSG-LSA, bei der Erstellung von Bürgerinformationen sowie bei allgemeinen Bürgereingaben und Anfragen zum Datenschutz

- Beteiligung bei der Konzeption und Auswertung von Protokolldateien mit Personenbezug

- Schulung der Mitarbeiter zu Fragen des Datenschutzes und der Datensicherheit

- regelmäßige oder gelegentliche Berichte an die Verwaltungsleitung über den Stand der Sicherstellung des Datenschutzes und der Datensicherheit innerhalb des Landkreises

- Zusammenarbeit mit dem IT-Sicherheitsbeauftragten

- ggf. Zusammenarbeit mit den Beauftragten für Datenschutz anderer Einrichtungen

- Zusammenarbeit mit dem Personalrat.

6.5 Aufgaben des Amtes für Recht und Kommunalaufsicht
Sofern sich Zweifel hinsichtlich der Auslegung der geltenden Rechtsvorschriften ergeben, ist das Amt für Recht und Kommunalaufsicht um gutachterliche Stellungnahme zu bitten. Anfragen sind über die Stabsstelle zu richten. Dadurch wird sichergestellt, dass generelle Zweifelsfragen erkannt und notwendige Regelungen für den gesamten Bereich der Verwaltung vorgenommen werden können.

6.6 Beteiligung an Arbeitskreisen
Die Beteiligung an überörtlichen Arbeitskreisen, an Arbeitsgemeinschaften und dergleichen für die Einführung und Weiterentwicklung von technikunterstützter Informationsverarbeitung ist anzustreben.

7. Beschaffung der Hard- und Software

7.1 Zuständigkeit
Den verantwortlichen Leitern der Organisationseinheiten des Landkreises Mansfeld-Südharz obliegen in Abstimmung mit den Zentralen Diensten/Sachgebiet EDV die Beschaffung der Hard- und Software sowie Erteilung von Aufträgen zu Wartungs- und sonstigen Leistungen auf dem Gebiet der Informations- und Kommunikationstechnik. Desweiteren erfolgt durch das Sachgebiet EDV die technische Übernahme (Installation) der Hardware und Implementierung der Software sowie die Leistungsabnahme nach Software-, Datenerfassungs- bzw. Datenverarbeitungsvergaben unter Hinzuziehung beteiligter Fachämter.

Nach Implementierung der Software ist der Beauftragte für den Datenschutz durch den Leiter der Organisationseinheit über den Einsatz zu informieren.

7.2 Benutzung fremder Datenverarbeitungsanlagen
Die Leiter der Organisationseinheiten regeln in Zusammenarbeit mit dem Sachgebiet EDV und dem Beauftragten für den Datenschutz die Vergabe von Aufträgen zur Verarbeitung personenbezogener Daten. Dabei sind der § 8 DSG-LSA sowie für die Sozialleistungsträger der § 80 SGB X unbedingt zu beachten; dies gilt auch für die Benutzung fremder Datenverarbeitungsanlagen im Störfalle.

Teil II

Durchführung automatisierter Verfahren

1. Gemeinsame Regelungen für zentrale und dezentrale IT-Verfahren

1.1 Begriffsbestimmungen
Zentrale IT-Verfahren sind solche, die auf einem Zentralrechner des Rechenzentrums (RZ) im Sachgebiet EDV oder im Rahmen der Auftragsdatenverarbeitung bei einem damit vertraglich

beauftragten Rechenzentrum datenverarbeitungstechnisch ablaufen.

Dezentrale IT-Verfahren sind solche, die mittels Informationstechnik der verantwortlichen Stelle, z.B. auf Mehrplatzsystemen, in lokalen Netzen (LAN) oder auf Einzelplatzrechnern unter datenverarbeitungstechnischer Eigenverantwortung der fachlich zuständigen Organisationseinheit ablaufen.

1.2 Benutzung der Informationstechnik

Die Informationstechnik (IT) **darf nur für dienstliche Zwecke** genutzt werden. Anträge auf Ausnahmen sind unter Angabe des Grundes, des Datenumfanges und der zeitlichen Dauer an das Sachgebiet EDV zu richten.

Den Benutzern steht die Anlage zur Verarbeitung in der Regel wochentags in der Zeit 6.00 - 20.00 Uhr zur Verfügung.

Abweichende Zeiten sind frühzeitig durch die Organisationseinheiten mit den Systemverwaltern abzustimmen. Die Benutzerzeiten können, soweit notwendig, verändert werden. Die Systemverwalter unterrichten die Leiter der Organisationseinheiten.
Bei den Verarbeitungszeiten hat das Sachgebiet EDV grundsätzlich die Aufsicht über die Benutzer.

1.3 Einrichtung von Bildschirmarbeitslätzen

Bei der Einrichtung von Bildschirmarbeitsplätzen legt soweit
- bauliche Veränderungen erforderlich sind - der Fachbereich 3 - Gebäudemanagment - im Zusammenwirken mit dem Hoch- und Tiefbauamt, dem Sachgebiet EDV, der Fachkraft für Arbeitssicherheit und der jeweiligen Organisationseinheit,

oder sonst
- das Sachgebiet Zentrale Dienste im Benehmen mit dem Sachgebiet EDV, der Fachkraft für Arbeitssicherheit und der verantwortlichen Organisationseinheit die notwendigen Maßnahmen im Hinblick auf die elektrische Versorgung, Beleuchtung, Raumausstattung und -einrichtung unter Beachtung der gesetzlichen und der in dieser Dienstanweisung getroffenen Regelungen fest.

1.4 Feststellung der Art der zu schützenden Daten

Vor dem Einsatz eines automatisierten Verfahrens ist
a) der Grad der Schutzbedürftigkeit der personenbezogenen Daten festzustellen,
b) eine Bedrohungs- und Risikoanalyse durchzuführen.
c) ein auf dem IT-Sicherheitskonzept basierendes Datensicherheitskonzept zu erstellen und umzusetzen sowie
d) eine entsprechende Kontrolle und Fortschreibung des Datensicherheitskonzeptes zu gewährleisten.

Diese Vorgehensweise ist auch Grundlage für die Verfahrensfreigabe und die Vorabkontrolle gemäß § 14 Abs. 2 DSG-LSA.

1.5 Technisch-organisatorische Maßnahmen zur Datensicherheit (Sicherheitsziele des DSG-LSA)

Bei der automatisierten Erhebung, Verarbeitung oder Nutzung sind Maßnahmen zu treffen, die je nach Art der zu schützenden Daten geeignet sind, zu gewährleisten, dass

1. diese nur Befugte zur Kenntnis nehmen können (Vertraulichkeit);
2. diese während der Erhebung, Verarbeitung und Nutzung unversehrt, vollständig und aktuell bleiben (Integrität);

3. diese zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet oder genutzt werden können (Verfügbarkeit);
4. diese ihrem Ursprung zugeordnet werden können (Authentizität);
5. festgestellt werden kann, wer wann welche Daten in welcher Weise erhoben, verarbeitet oder genutzt hat (Revisionsfähigkeit);
6. die Verfahren zur Erhebung, Verarbeitung oder Nutzung nachvollziehbar und aktuell dokumentiert sind (Transparenz).

Werden personenbezogene Daten nicht automatisiert erhoben, verarbeitet oder genutzt, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport oder der Vernichtung zu verhindern.

Die Maßnahmen zur Erreichung der Sicherheitsziele des DSG-LSA werden für jedes einzelne Verfahren vor der Verfahrensfreigabe vom Sachgebiet EDV unter Einbeziehung der verantwortlichen Organisationseinheit festgelegt und ist ebenfalls im Verfahrensverzeichnis Ziffer 9.1 zu dokumentieren.

1.6 Verfahrensfreigabe

Die Verfahrensfreigabe erfolgt nach den Prüfansätzen der **Anlage 5** und gilt für alle Programme, ohne Rücksicht darauf, wer die Programme erstellt hat.
Das Erwirken der Verfahrensfreigabe bei zentralen und dezentralen IT-Verfahren obliegt nach Antragstellung der verantwortlichen Organisationseinheit dem Sachgebiet EDV.

Die Verfahrensfreigabe umfasst
- die datenschutzrechtliche Freigabe bei automatisierten Verfahren mit personenbezogenen Daten,
- die fachliche Freigabe und
- die Anwendungsverfügung durch den Landrat.

Die datenschutzrechtliche Freigabe umfasst die Freigabe des erstmaligen Einsatzes von Datenverarbeitungsverfahren oder von wesentlichen Änderungen dieser Verfahren, nach Beratung durch den eingesetzten Beauftragten für den Datenschutz.

Mit der fachlichen Freigabe wird aufgrund von Testergebnissen bestätigt, dass das neue oder geänderte Programm bzw. Programmsysteme zur vorgesehenen ordnungsgemäßen Aufgabenerfüllung genutzt werden kann. Wird ein Datenverarbeitungsprojekt in Teilabschnitten realisiert, kann sich die Freigabe auf einzelne Teilabschnitte beziehen.

Die fachliche Freigabe ist von der Organisationseinheit zu erklären.

Beim Vorliegen einer Verfahrensfreigabe durch andere Stellen ist vor Inbetriebnahme durch das Rechnungsprüfungsamt, die Organisationseinheit, das Sachgebiet EDV und dem Beauftragten für den Datenschutz gemeinsam zu klären, ob Ziffer 1.5. und 1.6. anzuwenden ist.

1.7 Meldung bei erstmaligem Einsatz oder Änderung von automatisierten Verfahren

Die Erstellung, Ergänzung bzw. Änderung sowie der Einsatz neuer Verfahren ist im Verfahrensverzeichnis (§ 14 Abs. 3 DSG-LSA) zu dokumentieren.
Dazu hat die verantwortliche Organisationseinheit in jedem Fall eine Meldung an den Beauftragten für den Datenschutz nach dem Muster der **Anlage 5** einzuleiten.

1.8. Programmprüfung und Feststellung der Unbedenklichkeit
Soweit IT-Programme das Kassen- und Rechnungswesen berühren, sind diese Programme vor Einsatz durch das Rechnungsprüfungsamt zu prüfen und für unbedenklich zu erklären; dies gilt auch für alle Programmänderungen. Liegt eine Erklärung der Unbedenklichkeit durch eine andere Stelle bereits vor, entscheidet das Rechnungsprüfungsamt, ob Ziffer 1.5. anzuwenden ist.

1.9 Benutzung der Bildschirmgeräte
Bildschirmgeräte sind so aufzustellen, dass personenbezogene oder sonstige vertrauliche Daten, die auf dem Bildschirm angezeigt werden, von Unbefugten nicht eingesehen werden können. Ist dies aus räumlichen Gegebenheiten nicht möglich, so ist die Anzeige auf dem Bildschirm zu unterdrücken.

Bei Verlassen der Zimmer sind diese abzuschließen. Bei Arbeitsende ist zusätzlich die in Arbeit befindliche IT-Anwendung ordnungsgemäß abzuschließen und der Kleinrechner (PC) auszuschalten.

2. Spezielle Regelungen für zentrale IT-Verfahren

2.1 Regeln der kommunalen Datenzentralen oder beauftragten Rechenzentren (RZ)
Der Landkreis Mansfeld-Südharz nimmt im Rahmen der vom RZ vorgehaltenen Programme am Online-Vorgangsbearbeitungs- und -auskunftsverfahren teil. Die Durchführung dieser Verfahren hat nach den Regeln der Verfahrensanweisungen und der Anwendungshandbücher des RZ zu erfolgen.

2.2 Zugriffsberechtigung/Passwort-Vergabe
Das Zugriffsrecht zu den gespeicherten Datenbeständen ihres Fachbereiches haben grundsätzlich nur die zuständigen Organisationseinheiten. Das Zugriffsrecht kann für bestimmte Datenfelder, die dann schriftlich festgelegt werden müssen, auch einer anderen Organisationseinheit eingeräumt werden. Voraussetzung hierfür ist das Vorliegen der Nutzungsvoraussetzungen des § 10 DSG-LSA bzw. anderer Rechtsvorschriften i.S. des § 3 Abs. 3 DSG-LSA.

Bei den Sozialleistungsträgern ist das Zugriffsrecht zu den gespeicherten Daten grundsätzlich nur auf den Fachbereich begrenzt. Das Zugriffsrecht kann für bestimmte Datenfelder auch einem anderen Fachbereich der Organisationseinheit eingeräumt werden. Voraussetzung hierfür ist das Vorliegen der Nutzungsberechtigung nach § 67 b und c, SGB X bzw. anderer Rechtsvorschriften.

Zur Steuerung der Zugriffsberechtigung auf Datenbestände, die über Bildschirmgeräte abgerufen und verändert werden können (Online-Dialog), wird eine Sicherungsdatenbank im RZ vorgehalten. Sie enthält die Namen der zugriffsberechtigten Mitarbeiter/innen, den Umfang der Zugriffsberechtigung und eine Benutzerkennung zur Ausübung der Zugriffsberechtigung. Diese Sicherungsdatenbank wird vom jeweiligen Mitarbeiter des Sachgebietes EDV verwaltet, der für die Betreuung der EDV-Technik in diesem Bereich verantwortlich ist (Sicherheitsverwalter).
Dieser teilt den zugriffsberechtigten Mitarbeitern die von ihnen ausgewählte Benutzerkennung zu und legt in Absprache mit dem jeweiligen Leiter den Umfang der Zugriffsberechtigung (z.B. nur Auskünfte, Einschränkungen der Vorgangsbearbeitung) durch zusätzliche Information in der Sicherheitsdatei fest.

Anträge von Organisationseinheiten auf Zuteilung von Zugriffsberechtigungen auf Daten anderer Bereiche sind unter Einschaltung des Beauftragten für den Datenschutz an die zuständige Organisationseinheit zu richten.

2.3 Passwort-Vergabe
Die Eingabe und Änderung von Daten sowie die Erteilung von Auskünften aus den Datenbanken dürfen am Bildschirm nur Mitarbeiter vornehmen, die durch die Benutzerkennung eine Zugriffsberechtigung auf vorhandene Datenbestände haben.

Die Benutzerkennung wird durch das Passwort geschützt. Dieses ist von den Mitarbeitern geheim zu halten. Die Mitarbeiter haben in geeigneter Weise sicherzustellen, dass andere Personen das Passwort weder bei der Eingabe noch anderweitig bekannt wird.

Falls ein Mitarbeiter berechtigte Bedenken hat, dass sein Passwort bekannt geworden ist, hat er umgehend mit dem Sicherheitsverwalter der speichernden Stelle ein neues Passwort zu vereinbaren.

Besteht der begründete Verdacht, dass nach Bekanntwerden eines Passwortes der Datenbestand unberechtigt verändert wurde, hat der betroffene Mitarbeiter seinen Vorgesetzten und dieser den Beauftragten für den Datenschutz darüber zu informieren.

In Zusammenarbeit mit dem Sachgebiet EDV und dem Beauftragten für den Datenschutz hat die Organisationseinheit den betroffenen Datenbestand auf einen möglichen Missbrauch zu prüfen. Wird ein unberechtigter Eingriff festgestellt, sind unverzüglich der Leiter des betroffenen Fachbereiches und der Landrat zu beteiligen.

Ist es erforderlich, bei Abwesenheit eines Mitarbeiters mit dessen Benutzerkennung zu arbeiten, so ist durch den Administrator das Passwort zurückzusetzen. Nach Rückkehr des Mitarbeiters muss dieser das Passwort wieder ändern.

2.4 Passwort-Verwaltung
Für Vertretungs- oder Notfälle ist das Administrator-Passwort in einem Safe zu hinterlegen und dessen Benutzung ist zu protokollieren. Bei Benutzung durch Dritte ist es vom Administrator baldmöglichst wieder zu ändern, damit sichergestellt ist, dass es nur einer Person bekannt ist.

3. Gemeinsame Regelungen für dezentrale IT-Verfahren

3.1 Ordnungsgemäße Anwendung der Programme bei dezentraler Datenverarbeitung (§ 14 DSG-LSA)

Der Einsatz und der Umfang der Nutzung von Datenverarbeitungsprogrammen für die Informationsverarbeitung auf autonomen Systemen (z.B. Personalcomputer, Textverarbeitungssysteme) bedarf der vorherigen schriftlichen Genehmigung der Zentralen Verwaltung - Sachgebiet EDV.
Die Überwachung der ordnungsgemäßen Anwendung dieser Datenverarbeitungsprogramme obliegt den zuständigen Leitern der Organisationseinheiten.

3.2 Einsatz der Software
Für dezentrale IT-Verfahren dürfen **nur** die vom Sachgebiet EDV bestimmten Betriebssysteme und

die gemeinsam mit der Organisationseinheit ausgewählte Software eingesetzt werden.

3.3 Festlegungen der zu verarbeitenden Daten
Beim erstmaligen Einsatz von dezentralen IT-Verfahren sind die zu speichernden Daten und die weiteren Verarbeitungsschritte gemeinsam vom Sachgebiet EDV und vom verantwortlichen Bereich unter Beteiligung des Beauftragten für den Datenschutz festzulegen.

3.4 Ausweiten der Informationsverarbeitung
Wenn die Organisationseinheit beabsichtigt, die Informationsverarbeitung über den ursprünglich genehmigten Umfang hinaus auszudehnen, ist **vorher** die Zustimmung des Sachgebietes EDV unter Beteiligung des Beauftragten für den Datenschutz einzuholen.

3.5 Gewährleistung Wartung und Störungsbeseitigung
Die Organisationseinheiten unterrichten den Fachdienst EDV unverzüglich über auftretende Störungen.
Für die Datenverarbeitungsanlagen und die Datensichtgeräte gelten für die Störungsbeseitigung während der Gewährleistungsfrist die bei der Beschaffung vereinbarten Bedingungen.
Für die Wartung nach der Gewährleistungsfrist gelten die mit dem Hersteller- bzw. Lieferfirmen abgeschlossenen Wartungsverträge.

Von Seiten des Sachgebietes EDV ist darauf zu achten, dass die Reparaturtätigkeit in angemessenem Zeitraum (ca. 4 Std.) nach der Verständigung beginnt und zügig abgeschlossen wird.

Die einzelnen Organisationseinheiten sind von größeren terminlichen Verzögerungen wegen technischer Störungen oder aus anderen Gründen **rechtzeitig** vom Sachgebiet EDV zu benachrichtigen.

Alle Gerätestörungen sind in einen sogenannten Störungsnachweis einzutragen. In diesem Störungsnachweis der im Sachgebiet EDV geführt wird, hat das Wartungspersonal nach Durchführung der Arbeiten zu bestätigen, dass die Betriebssicherheit der Anlage oder Geräte wiederhergestellt wurde.

Die Störungsbeseitigung unter Nutzung des Zugriffsrechtes des Systemverwalters und bei Beendigung des Zugriffes ist dem Betreiber der Anlage anzuzeigen.

Bei der Wartung und Reparatur von DV-Anlagen sollte der Zugriff Dritter auf personenbezogene Daten möglichst vermieden werden. Ist dies nicht möglich, so ist § 8 Abs. 7 DSG LSA zu beachten.

3.6 Technische Arbeitsabwicklung
Bei der technischen Abwicklung von Datenverarbeitungsverfahren ist durch das Sachgebiet EDV sicherzustellen, dass

- für Arbeiten, die nicht nur zur Probe durchgeführt werden, nur die zuletzt freigegebenen Programme (Revisionsstand) zu verwenden sind,
- nicht mehr aktuelle Programme in einer besonderen Programmbibliothek archiviert werden,
- nachgewiesen wird, welches Programm für welche Arbeit eingesetzt wurde,
- Datenbestände eindeutig gekennzeichnet und Sicherungsmöglichkeiten ausgenutzt werden,
- durch programmierte Plausibilitätskontrollen die Richtigkeit der Daten weitestgehend gewährleistet ist,
- durch entsprechende Wiederanlaufroutinen Systemzusammenbrüche usw. schnell überbrückt

werden können,

- die Funktionsfähigkeit der Datenverarbeitungsanlagen und der Datenstationen gewährleistet ist,
- die notwendigen Wartungsarbeiten erfolgen,
- Unbefugte sich nicht in den Besitz von Daten bringen können und
- größtmögliche Sicherheit gewährleistet ist;

3.7 Datensicherheit
Durch das Sachgebiet EDV ist in Zusammenarbeit mit den dafür verantwortlichen Organisationseinheiten durch organisatorische, technische und bauliche Maßnahmen sicherzustellen, dass das gesamte Datenverarbeitungssystem einschließlich Daten- und Programmbestand vor Zerstörung, unsachgemäßer Behandlung, unberechtigter Verwendung u.ä. gesichert ist.(siehe auch § 6 Abs. 2 und 3 DSG-LSA, Teil II, Ziffer 1.5. dieser Dienstanweisung)

3.8 Datensicherung
Die Datenträger sind zu kennzeichnen, in feuersicheren Data-Safes der Güteklasse S 60 DIS oder S 120 DIS nach RAL RG 626/7 sicher zu verwahren und in einem gesonderten Verzeichnis nachzuweisen.

Die Aufbewahrung der Datenträger erfolgt in der Regel in Form des Drei-Generations-Prinzips, damit bei Verlust eine Rekonstruktion jederzeit möglich ist.

Darüber hinaus ist eine Gesamtsicherung wöchentlich auszulagern.

Datenträger, die an Dritte weitergegeben werden, sind nach Maßgabe der Datenübermittlungsgrundsätze mit Ausgangsdatum und Empfänger in einem Nachweis zu registrieren. Ebenfalls ist der Zeitpunkt und die Art der Rücksendung darin zu vermerken.

4. Spezielle Regelungen für den Einsatz von Einzelplatzrechnern (PC)

4.1 Einzelplatzrechner (PC)
Die Kleinrechner werden von den Organisationseinheiten eigenverantwortlich betrieben.

Die Organisationseinheit benennt dem Sachgebiet EDV einen verantwortlichen Mitarbeiter für jeden eingesetzten PC.

Die verantwortlichen Mitarbeiter stellen sicher, dass
- ausschließlich das vom Sachgebiet EDV bestimmte Betriebssystem und die gemeinsam ausgewählte Software eingesetzt wird,
- ausschließlich die beim erstmaligen Einsatz des Datenverarbeitungssystems festgelegten Daten sowie die evtl. beantragte und genehmigte Datenerweiterung gespeichert und verarbeitet werden,
- die urheberrechtlichen Bestimmungen beachtet werden,
- die erforderlichen Wartungsarbeiten durchgeführt werden,
- alle einschlägigen Datenschutz- und Datensicherheitsbestimmungen angewandt werden.

Das Sachgebiet EDV stellt unter Einbeziehung des Betreibers sicher, dass
- die urheberrechtlichen Bestimmungen beachtet werden,
- die erforderlichen Wartungsarbeiten durchgeführt werden,
- die einschlägigen Datensicherungsbestimmungen angewandt werden,
- keine Installation von nicht freigegebener Software erfolgt.

4.2 Datensicherheit beim Einsatz von PC
Die Datensicherheit ist durch Anwendung von software- und hardwaremäßigen Sicherheitsprodukten entsprechend den Anforderungen nach der Sensibilität der personenbezogenen Daten zu gewährleisten.

Näheres ergibt sich aus den Verwaltungsvorschriften zu § 6 DSG-LSA. Die nach § 6 Abs. 2 und 3 DSG-LSA zu treffenden technisch-organisatorischen Maßnahmen sollten insbesondere unter Beachtung der Risiken des Einsatzes von Einzelplatzrechnern und den darauf eingesetzten Betriebssystemen erfolgen.(siehe auch Teil II, Ziff. 1.5 dieser Dienstanweisung)

Die zu veranlassenden technisch-organisatorischen Maßnahmen bei den Sozialleistungsträgern sind nach § 78a SGB X i.V. mit der Anlage zu § 78a zu beurteilen.

4.3 Datensicherung beim Einzelplatzrechner
Backub-Datenträger sollten grundsätzlich in feuersicheren Data-Safes der Güteklasse S 60 DIS oder S 120 DIS nach RAL RG 626/7 aufbewahrt werden.Damit werden hitze- und feuchtigkeits-empfindliche Datenträger, wie z.B. Disketten 60 bzw. 120 Minuten vor Zerstörung geschützt.
Die erforderliche Datensicherung ist durch den Betreiber in Zusammenarbeit mit dem Fachdienst EDV sicherzustellen. Den Umfang legt der Betreiber fest.

Teil III

Richtlinien für die Durchführung von Projekten (Projektrichtlinien)

1. Zielsetzung
(1) Diese Richtlinien sollen ein einheitliches Vorgehen bei der Planung und Ausführung von Projekten sicherstellen. Sie sollen
a) das angemessene Verhältnis zwischen Aufwand und Nutzen einer Anwendung,
b) die Transparenz der Vorgehensweise,
c) eine rationelle Projektplanung und -sicherung,
d) eine projektbegleitende Dokumentation,
e) die Prüfbarkeit des Projektes auf Zweckmäßigkeit und Wirtschaftlichkeit,
f) die Beachtung des Datenschutzes und
g) die Beteiligung der Bediensteten und der Personalvertretung am Projekt
gewährleisten.

2. Projektauftrag
(1) Dem Projektträger ist ein schriftlicher Auftrag zu erteilen (Projektauftrag).

(2) Im Projektauftrag sind insbesondere festzulegen
- Bezeichnung und Zielsetzung des Projektes,
- Inhalt und Umfang
- Rahmenbedingungen oder Auflagen
- Schnittstellen und Berührungspunkte zu anderen Projekten
- Personal- und Sachmittelauslastung,
- Zeitrahmen,
- Projektorganisation

- Projektberichterstattung.

(3) Beabsichtigt der Projektträger, von den Vorgaben des Projektauftrages abzuweichen, so ist die Entscheidung des Auftraggebers herbeizuführen.

(4) Über bedeutende Projekte, bei denen personenbezogene Daten verarbeitet werden sollen, sowie über grundlegende Änderungen solcher Verfahren sollte der Landesbeauftragte für den Datenschutz in Anlehnung an § 22 Abs. 4 Satz 2 DSG-LSA frühzeitig unterrichtet werden.

(5) Soll das Projekt durch externe kostenpflichtige Beratung ergänzt werden, so bedarf dies der Zustimmung des Auftraggebers.

3. Phasenkonzept
(1) Projekte sind grundsätzlich in den Phasen
- Projekt-Untersuchung und
- Projekt-Ausführung
abzuwickeln. Projekten mit hoher Komplexität sollte eine Voruntersuchung vorausgehen.

(2) Die Projekt-Untersuchung kann in begründeten Fällen verkürzt werden. Gründe können insbesondere das Vorliegen dokumentierter Erkenntnisse zum Untersuchungsziel oder die Mitarbeit in einem Entwicklungsverbund sein. Die Gründe sind zu dokumentieren.

4. Voruntersuchung
(1) Die Voruntersuchung soll es zulassen, das Projekt unter technischen, wirtschaftlichen und organisatorischen Gesichtspunkten zu beurteilen.

Die Ergebnisse der Voruntersuchung sind in einem Bericht darzustellen, der insbesondere enthalten soll:
- Beschreibung, Analyse und Bewertung des Ist-Zustandes aufgrund einer groben Aufgabenuntersuchung,
- Beschreibung der Lösungsvarianten mit einer Grobplanung für ihre Ausführung,
- vergleichbare Bewertung der Lösungsvarianten mit einer Wirtschaftlichkeitsbetrachtung,
- Hinweise auf Schnittstellen und Berührungspunkte zu anderen Projekten,
- Entscheidungsvorschlag für das weitere Vorgehen.

(2) Der Auftraggeber entscheidet aufgrund des Voruntersuchungsberichtes, ob- und ggf. für welche Lösungsvariante - eine Projekt-Untersuchung durchgeführt werden soll.

5. Projekt-Untersuchung
(1) Zweck der Projekt-Untersuchung ist es, die technischen Anforderungen an den Technikeinsatz im einzelnen festzulegen, ein Sollkonzept auszuarbeiten und dessen Wirtschaftlichkeit eingehend zu überprüfen. Die Ergebnisse der Projekt-Untersuchung sind in einem Bericht darzustellen. Er sollte eine Kurzfassung enthalten.

(2) Der Bericht über die Projekt-Untersuchung soll insbesondere enthalten:
a) Beschreibung, Analyse und Bewertung des Ist-Zustandes aufgrund einer Aufgabenuntersuchung und/oder einer Kommunikationsanalyse

b) Beschreibung des Sollkonzeptes mit Aussagen zu
- dem technischen Konzept
- der Aufbau- und Ablauforganisation

- den Leistungsanforderungen an Geräte und Programme

- den Maßnahmen zur Datensicherheit und zum Datenschutz
- den Schnittstellen zu anderen Verfahren und Projekten und
- den erforderlichen Einführungsmaßnahmen (Schulung, Anwender- und Systembetreuung)

c) Angaben zu den für die Ausführung erforderlichen Personal- und Sachmittel

d) Schätzung der erforderlichen Personal- und Sachmittel für den laufenden Betrieb

e) Wirtschaftlichkeitsuntersuchungen

f) Darstellung der positiven und negativen Auswirkungen des Vorhabens einschließlich der Sozialverträglichkeit

g) Arbeits- und Zeitplan und

h) Entscheidungsvorschlag für das weitere Vorgehen.

(3) Von der theoretischen Untersuchung nach den Absätzen 1 und 2 kann abgewichen werden, wenn sich die erforderlichen Aussagen nur treffen lassen, indem zunächst Lösungsansätze in einem eingegrenzten Bereich stufenweise entwickelt und erprobt werden (sog. prototyping)

(4) Der Auftraggeber entscheidet aufgrund des Projektuntersuchungsberichtes über die Ausführung des Soll-Konzepts.

6. Projekt-Ausführung

(1) Die Projekt-Ausführung setzt die Entscheidung über die Projekt-Untersuchung (Nr. 5 Abs. 4) voraus. Die Projektausführung umfasst insbesondere die Beschaffung der Geräte und Programme sowie die erforderlichen Einführungsmaßnahmen entsprechend dem Soll-Konzept.

(2) Ist die Entwicklung von Anwendersoftware erforderlich, ergänzt sich die Ausführungsphase um die Abschnitte
- Detailorganisation
- Softwareerstellung
- Test und Freigabe

7. Detailorganisation

Im Abschnitt Detailorganisation sind auf der Grundlage des Soll-Konzepts alle Fragen der Programmgestaltung einschließlich der organisatorischen Veränderungen vollständig darzustellen. Die Detailorganisation umfasst insbesondere

- Festlegung der manuellen und maschinellen Arbeitsabläufe
- Erstellung der für den Verfahrensablauf erforderlichen Regelungen
- Beschreibung der einzusetzenden Hardware und Systemsoftware
- vollständige Ausgestaltung der Datenorganisation einschl. der Maßnahmen für die Verfahrenssicherheit und den Datenschutz
- Ausarbeitung der Vorgaben bzw. der Leistungsbeschreibung für die Softwareerstellung
- Festlegen der Schnittstellenbedingungen
- Vorbereitung der Testarbeiten und
- Planung der Einführungsmaßnahmen.

8. Erstellen von Anwendungssoftware
Die Anwendungssoftware ist nach den Programmiervorgaben der Detailorganisation zu erstellen. Die Programmierung soll grundsätzlich in einer problemorientierten und genormten Programmiersprache erfolgen. Um eine rationelle Programmentwicklung und -pflege sicherzustellen, sollen möglichst standardisierte Methoden für Softwareentwicklung und -dokumentation angewendet werden.

9. Test und Freigabe
(1) Anwendungssoftware ist vor ihrem Einsatz umfassend zu testen. Sie darf erst eingeführt werden, wenn sie förmlich freigegeben ist. Die Freigabe setzt einen beanstandungsfreien Test sowie das Vorliegen der Programmdokumentation voraus.

(2) Mit der Freigabe wird die Verantwortung übernommen, dass die für die Ordnungsmäßigkeit und Sicherheit des rechnergestützten Verfahrens erforderlichen Maßnahmen getroffen sind.

(3) Absatz 1 gilt auch für Anwendungssoftware, die von Dritten erstellt worden ist.

10. Beschaffung von Geräten und Programmen
(1) Die projektbezogenen Anforderungen an die zu beschaffenden Geräte und Programme sind vor Einleitung von Beschaffungsmaßnahmen in einem Pflichtheft zu formulieren.

(2) Die für das öffentliche Beschaffungswesen (VOL) verbindlichen Vergabebestimmungen einschließlich der Besonderen Vertragsbedingungen (BVB) sind zu beachten oder gegebenenfalls zu vereinbaren.

11. Wirtschaftlichkeitsuntersuchungen
(1) Um die Wirtschaftlichkeit eines Projektes beurteilen zu können, ist es erforderlich,
- die damit verbundenen Kosten zu ermitteln,
- den damit einhergehenden Nutzen darzustellen sowie
- Kosten und Nutzen gegeneinander abzuwägen oder bei Alternativen mit gleichem Nutzen die Kosten zu vergleichen.

(2) Welche Methode bei der Wirtschaftlichkeituntersuchung anzuwenden ist, hängt im Einzelfall vom Projektauftrag und der Möglichkeit ab, Kosten zu ermitteln und den Nutzen in Geld zu bewerten.

(3) Bei der Durchführung von Wirtschaftlichkeitsuntersuchungen ist darauf zu achten, dass der Aufwand dafür in einem angemessenen Verhältnis zur Aussagekraft und zum Erkenntniswert steht.

12. Dokumentation
(1) Die Durchführung des Projekts muss durch Unterlagen nachvollziehbar belegt sein (Projektdokumentation). Die Projektdokumentation ist projektbegleitend zu erstellen. Sie muss für sachkundige Dritte verständlich und prüffähig sein. Der Projektträger ist für die Projektdokumentation verantwortlich.

(2) Wird anwendungsbezogene Software erstellt oder geändert, so ist sie ausreichend zu dokumentieren (Projektdokumentation). Zur Programmdokumentation gehören mindestens:
- Beschreibung der Aufgabenstellung und der Arbeitsabläufe einschl. der Kontrollen,
- Darstellung der Daten- und datenflussorganisation,

- Arbeitsanweisungen
  . für die betroffenen Fachbereiche,
  . für den Rechenzentrumsbetrieb,
- Programmvorhaben (Detailorganisation),
- Quellprogramme,
- Beschreibung der Maßnahmen zur Verfahrenssicherheit und zum Datenschutz
- Darstellung der Tests und der Ergebnisse und
- Freigabeerklärung.

13. Dateifestlegung
Die Errichtung einer Datei über personenbezogene Daten bedarf der besonderen Festlegung. Diese muss mindestens die nach § 14 Abs. 2 Satz 2 DSG-LSA genannten Merkmale enthalten.

14. Standards und Normen
Bei der Planung und Ausführung von Projekten sind die verbindlichen Normen, Standards und Empfehlungen für den Einsatz der IuK-Technik zu beachten. Das gleiche gilt für den EG-Ratsbeschluss (87/95/EWG) vom 22.12.1986 über die Normierung im Bereich der Informationstechnik und der Telekommunikation (EG-Amtsblatt Nr. L 36/31 vom 07.02.1987).

15. Mitgestaltung des IT-Technikeinsatzes am Arbeitsplatz
Den von einem Projekt betroffenen Bediensteten ist in geeigneter weise Gelegenheit zu geben, an der organisatorischen Gestaltung des IT-Technikeinsatzes an ihren Arbeitsplätzen mitzuwirken.

16. Beteiligung der Personalräte
Die zuständige Personalvertretung ist im Rahmen des Landespersonalvertretungsgesetzes an Projekten zu beteiligen.

Teil IV

Schlussbestimmungen
1. Alle Mitarbeiterinnen und Mitarbeiter tragen in ihrem Zuständigkeitsbereich die **Verantwortung** für die vollständige und korrekte Anwendung der geltenden Regelungen, Anweisungen und Vorschriften zur Gewährleistung von Datenschutz und Datensicherheit.

2. Diese Dienstanweisung tritt am 01.07.2008 in Kraft. Gleichzeitig tritt die Dienstanweisung Datenschutz und Datensicherheit für den Landkreis Mansfelder Land außer Kraft.

gez. Dirk Schatz
Landrat

Anlage 1 zur Dienstanweisung Datenschutz und Datensicherheit

Sicherheitsbelehrung für die Benutzung von Personalcomputern

Frau/Herr ..... wurde heute über die besonderen Risiken informiert, die bei der Benutzung eines Personalcomputers im Zusammenhang mit der Verarbeitung personenbezogener Daten entstehen können und ergänzend zur Dienstanweisung vom .....2008 auf die Einhaltung, insbesondere der folgenden technisch-organisatorischen Erfordernissen hingewiesen.

Die/Der Benutzer(in) wurde darüber belehrt, dass sie/er

- zur Verarbeitung personenbezogener Daten ausschließlich Verfahren einsetzen darf, die vor- und freigegeben sind,
- ausschließlich die vorgegebene Hard- und Software verwenden darf (der Einsatz privater Hardware und privater, nicht freigegebener, unlizenzierter und selbsterstellter Software sowie von Public Domain Programmen - frei verfügbarere kostenlose Software - und Shareware - Prüf-vor-Kauf-Software - sind untersagt),
- an der bereitgestellten Hardware keinerlei Veränderungen vornehmen darf,
- Verfahren (Programme, Software) und Daten nicht verfälschen und unbefugt an Dritte weitergeben darf,
- den Personalcomputer und die darauf gespeicherten Verfahren (Programme, Software) und Daten nur zur Erfüllung der vorgegebenen Aufgaben verwenden darf,
- die vorgegebenen Sicherheitsmaßnahmen zum Zugangs- und Zugriffsschutz sowie zum Virenschutz anzuwenden und einzuhalten hat,
- das Passwort keinem Dritten zur Kenntnis zu geben hat,
- den Internet-Zugang nur für dienstliche Zwecke nutzen darf,
- im Stand-alone-Betrieb des Personalcomputers zur Durchführung regelmäßiger Datensicherungen und für die zugriffssichere Aufbewahrung der Sicherungsdatenträger verantwortlich ist,
- personenbezogene Daten auf einem tragbaren Personalcomputer (Laptop, Notebookk) nur verschlüsselt speichern darf,
- zur Duldung der Revision durch dazu berechtigte Personen (Datenschutzbeauftragter, Benutzerservice) verpflichtet ist sowie alle sonstigen vorgegebenen technischen und organisatorischen Maßnahmen anzuwenden und einzuhalten hat,

um den Erfordernissen des Datenschutzes Rechnung zu tragen.

Bei Verstößen gegen diese Belehrung können ggf. arbeits- und im Rahmen der Strafgesetze auch strafrechtlich verfolgt und geahndet werden. Sie können auch Anlass einer außerordentlichen Kündigung sein.

Ort, Datum .....

....

Leiter/Beauftragter der Organisationseinheit Benutzer/in

Anlage 2 zur Dienstanweisung Datenschutz und Datensicherheit

Vernichtung von Datenträgern

1. Allgemeines
Ein Datenträger ist ein Mittel, auf dem Daten aufgezeichnet werden können. Datensicherungsmaßnahmen sind für Datenträger zu treffen, auf denen personenbezogene Daten oder vertrauliche Sachdaten aufgezeichnet sind. Datenträger sind bei automatisierter Datenverarbeitung sowohl die verarbeitbaren Datenträger (z.B. Magnetbänder, Magnetplatten, Disketten, Kassetten, optisch lesbare Belege) als auch die dabei erstellten Datenträger (z.B. Ausdrucke, Mikrofilmausgaben einschließlich ihrer Kopien). In nichtautomatisierten Verfahren können Datenträger z.B. sein: Karteikarten, Formblätter, Briefe, Vermerke, Notizen usw.

Grundsätzlich gilt, dass die Vernichtung der Daten dann anstehen, wenn die Aufbewahrungsfristen dem nicht entgegenstehen und keine Archivierung, z.B. nach §§ 9, 11 ArchG-LSA vorgenommen werden.

2. Sicherungsziel
Sind Datenträger zu vernichten, dann ist zu gewährleisten, dass sie tatsächlich vernichtet werden und nicht in die Hände Unbefugter fallen. Auf die DIN 32 757 wird hingewiesen.

3. Vernichtungsmaßnahmen
Die Organisationseinheiten haben unter Beachtung wirtschaftlicher Gesichtspunkte und des in § 6 Abs. 1 DSG festgeschriebenen Angemessenheitsgrundsatzes die erforderlichen Maßnahmen zur Vernichtung von Datenträgern zu wählen.
Als Maßnahme kommen in Frage:
- Verbrennen, Reißwolf
- chemische oder physikalische Vernichtung
- Übergabe an zuverlässige Unternehmen.

Die tatsächliche Vernichtung der Datenträger ist zu protokollieren. Es sind Vernichtungsprotokolle anzufertigen. Der Nachweis ist im Sachgebiet Zentrale Dienste zu führen.

4. Standorte für Einrichtungen zur Vernichtung
Es stehen zur Zeit bei folgenden Organisationseinheiten Einrichtungen für die Vernichtung von Datenträgern zur Verfügung:
- 1 Stück 250 l Sicherheitsbehälter, Standort Sangerhausen, Rudolf-Breitscheid-Str. 20/22, Haus 1
- 5 Stück 500 l Sicherheitsbehälter, Standort Sangerhausen, Rudolf-Breitscheid-Str. 20/22, Hausmeisterwerkstatt
- 1 Stück 500 l Sicherheitsbehälter, Standort Sangerhausen, Rudolf-Breitscheid-Str. 20/22, Haus 2
- 1 Stück 500 l Sicherheitsbehälter, Standort Sangerhausen, Rudolf-Breitscheid-Str. 20/22, Haus 3
- 1 Stück 500 l Sicherheitsbehälter, Standort Sangerhausen, Schartweg, Garage
- 1 Stück 70 l Sicherheitsbehälter T 7, Standort Sangerhausen, Thälmannstraße 30
- 1 Stück 250 l Sicherheitsbehälter, Standort Sangerhausen, Thälmannstraße, Ordnungsamt,
- 1 Stück 250 l Sicherheitsbehälter, Standort Sangerhausen, Medizinisches Zentrum, Bahnhofstraße 33, Rechnungsprüfungsamt
- 1 Stück 600 l Sicherheitsbehälter T 61 Standort Lutherstadt Eisleben, Größlerstraße 2
- 1 Stück 600 l Sicherheitsbehälter T 61 Standort Lutherstadt Eisleben, Karl-Fischer-Straße 13, Haus 6

- 2 Stück 600 l Sicherheitsbehälter T 61
- 1 Stück 250 l Sicherheitsbehälter T 23
- 5 Stück 70 l Sicherheitsbehälter T 7
  Standort Lutherstadt Eisleben, Lindenallee 56, Datenvernichtung
- 1 Stück 600 l Sicherheitsbehälter T 61
  Standort Lutherstadt Eisleben, Lindenallee 56, Haus 2

Die Benutzung dieser Einrichtungen durch die Organisationseinheiten ist jederzeit möglich.
Es ist vorher zu prüfen, ob wegen des Umfanges des zu vernichtenden Materials oder seines Inhalts andere Lösungen zweckmäßiger sind.

5. Zuständigkeitsregeln

Grundsätzlich sind die Organisationseinheiten für die Vernichtung von Datenträgern, die in ihrem Bereich entstehen bzw. anfallen, zuständig.

Fallen größere Mengen Datenträger aus Papier zur Vernichtung an und ist die Vernichtung durch eigenes Personal und Gerät unwirtschaftlich, ist das Sachgebiet Zentrale Dienste einzuschalten. Das Sachgebiet Zentrale Dienste beauftragt nach Klärung der Einzelheiten eine Firma mit der Vernichtung. Die Firma ist zur Abgabe einer Vernichtungsbestätigung zu verpflichten.

EDV-Technik, Festplatten, Disketten, Magnetplatten etc. sind beim Sachgebiet EDV abzugeben. Dort sind geeignete Behälter vorzuhalten, in denen die Datenträger bis zur Vernichtung gelagert werden.

In besonderen Fällen (z.B. gesetzlich geforderte aktenkundige Vernichtung) haben die Organisationseinheiten das Sachgebiet Zentrale Dienste zu informieren.

Die Vernichtung von Datenträgern außerhalb der Organisationseinheit darf nur in Abstimmung mit dem Sachgebiet Zentrale Dienste, Fachbereich 1 erfolgen. Dieses benennt die geeignete Firma.

Das Sachgebiet Zentrale Dienste sorgt im Zusammenwirken mit dem Beauftragten für den Datenschutz dafür, dass bei Einschaltung eines Auftragnehmers, der nicht in den Anwendungsbereich des DSG-LSA fällt, der Pflicht zur Unterrichtung des Landesbeauftragten für den Datenschutz nach § 8 DSG-LSA nachgekommen wird.

Anlage 3 zur Dienstanweisung Datenschutz und Datensicherheit

Landkreis Mansfeld-Südharz
Sachgebiet EDV

Freigabe des DV-Verfahrens/Programms
.....

Aufgrund der Ergebnisse der Verfahrensprüfung

( ) wird die Genehmigung zum Einsatz des Programms bzw. des Verfahrens erteilt
Unabhängig davon sind folgende Mängel baldmöglichst auszuräumen, **Anlage**

( ) wird die Genehmigung zum Einsatz des Programms bzw. des Verfahrens nicht erteilt.
Folgende Mängel stehender Verfahrensfreigabe entgegen: **Anlage**

Eine Stellungnahme des Personalrates

( ) liegt vor

( ) ist nicht erforderlich.

Datenschutzrechtliche Freigabe: .....
Datum Unterschrift

Fachliche Freigabe: .....
Datum Unterschrift

Verfahrensfreigabe: .....
Datum Unterschrift

Anlage 4 zur Dienstanweisung Datenschutz und Datensicherheit

Verfahrensverzeichnis nach § 14 Abs. 3 Satz 1 DSG-LSA

Verantwortliche Stelle 1	Stand vom:

1. Bezeichnung des Verfahrens 2
2. Zweckbestimmung 3 und Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung 4 (Die Zwecke und Rechtsgrundlagen vorgesehener Übermittlungen sind unter 5. angegeben)
3. Kreis der Betroffenen 5

□ Vorabprüfung nach § 14 Abs. 2 DSG-LSA erfolgt, weil

- □ es sich um ein Abrufverfahren nach § 7 Abs. 1 DSG-LSA handelt
- □ personenbezogene Daten besonderer Art (§ 2 Abs. 1 Satz 2 DSG-LSA erhoben, verarbeitet oder genutzt werden
- □ das Erheben, Verarbeiten oder Nutzen dazu bestimmt ist, die Persönlichkeit der oder des Betroffenen zu bewerten (§ 4a Abs. 1 DSG-LSA)
- □ mobile personenbezogene Datenträger (§ 2 Abs. 11 DSG-LSA) eingesetzt werden.

.....
Datum/Unterschrift (der für die Erstellung/Änderung verantwortlichen Person)

4. Art der Daten 6

5./6. vorgesehene Empfänger 7	Zweck 8	Weitergabe oder Übermittlung Rechtsgrundlage 9	Anlass und Häufigkeit	
a) innerhalb der verantwortlichen Stelle				
b) bei Übermittlung (auch in Drittländer) aa)im Inland, innerhalb der EU oder des Europäischen Wirtschaftsraums 10 bb)in Drittländer (stets erfüllt bei Einstellung ins Internet 10				
c) bei Erhebung, Verarbeitung oder Nutzung				

7. Regelfristen für 12

a) die Löschung

b) die Prüfung der Erforderlichkeit der weiteren Speicherung

8. Zugriffsberechtigte 13
(bitte erläutern)

9.1 Maßnahmen nach § 6 Abs. 2 DSG-LSA 14 zur Gewährleistung der		Dienstanweisung liegt bei ☐
Vertraulichkeit	Art der Maßnahme (bitte erläutern)	
Integrität	Art der Maßnahme (bitte erläutern)	
Verfügbarkeit	Art der Maßnahme (bitte erläutern)	
Authentizität	Art der Maßnahme (bitte erläutern)	
Revisionsfähigkeit	Art der Maßnahme (bitte erläutern)	
Transparenz	Art der Maßnahme (bitte erläutern)	

9.2 Art der Geräte (Hardware) [15] (bitte erläutern)

□ Großrechner:

□ Server:

□ Client:

□ Einzelplatzsystem:

9.2.1 Art der Geräte (Hardware) zum Anschluss an Fremdnetze [16] (bitte erläutern)

□ kein Anschluss an Fremdnetze

□ Intranet (z.B. Landesnetz)

□ Internet

9.2.2 Verfahren zur Übermittlung (bitte erläutern)

□ leitungsgebunden □ Funk □ Disketten □ Kassette (Streamer) □ Magnetband □ Sonstige (bitte erläutern)

9.3 eingesetzte Software (Betriebssysteme; Anwendungssoftware) [17] (bitte erläutern)

□ Großrechner:

□ Server:

□ Client:

□ Einzelplatzsystem:

9.3.1 eingesetzte Software zum Anschluss an Fremdnetze [18] (bitte erläutern)

□ kein Anschluss an Fremdnetze

□ Intranet (z.B. Landesnetz)

□ Internet

9.3.2 Verfahren zur Sperrung von personenbezogenen Daten

□ nicht vorhanden □ vorhanden (bitte erläutern)

9.3.3 Verfahren zur Löschung von personenbezogenen Daten

□ nicht vorhanden □ vorhanden (bitte erläutern)

Ausfüllanleitung

Das Verfahrensverzeichnis entfällt insbesondere bei:

§ 3 Abs. 2 Nr. 2 DSG-LSA	für öffentlich-rechtliche Kreditinstitute und Versicherungsanstalten
§ 3 Abs. 2 Nr. 3 DSG-LSA	bei Ausübung des Gnadenrechts
§ 14 Abs. 4 Nr. 1 DSG-LSA	für durch Rechtsvorschrift vorgeschriebene Register
§ 14 Abs. 4 Nr. 2 DSG-LSA	für Verfahren, die ausschließlich der Unterstützung der allgemeinen Bürotätigkeit dienen

Bereichsspezifische Regelungen, z.B. über Errichtungsanordnungen nach § 490 StPO, bleiben unberührt, ebenso für Festlegungen öffentlicher Stellen von Sozialversicherungsträgern und ihren Verbänden nach § 81 Abs. 4 Satz 1 SGB X i.V.m. Satz 1 und § 18 Abs. 2 Satz 2 BDSG.

1	Verantwortliche Stelle:	a) ist grundsätzlich die jeweilige öffentliche Stelle (§ 2 Abs. 8 DSG-LSA) (z.B. Regierungspräsidium, Landkreis, Gemeinde) b) nicht der Auftragnehmer bei einer Auftragsdatenverarbeitung Wird die Festlegung für das Verfahrensverzeichnis gemäß § 14 Abs. 3 Satz 2 DSG-LSA zentral getroffen, sind alle verantwortlichen Stellen, die das Verfahren anwenden, mit genauer Anschrift zu bezeichnen. Der jeweilige Beauftragte für den Datenschutz erhält eine Ausfertigung des Verfahrensverzeichnisses. Das Verfahrensverzeichnis soll die Organisationseinheit bezeichnen, die innerhalb der jeweiligen verantwortlichen Stelle intern verantwortlich ist.
2	Bezeichnung des Verfahrens:	a) hier ist der Name des Verfahrens anzugeben (z.B. Einwohnermeldedaten) b) bei landeseinheitlichen DV-Verfahren ist deren Bezeichnung anzugeben
3	Zweckbestimmung:	der Zweck der Erhebung, Verarbeitung oder Nutzung (ohne Übermittlungen) ist kurz zu erläutern
4	Rechtsgrundlage der Erhebung, Verarbeitung oder Nutzung:	mit Angabe der Paragraphen der einschlägigen Rechtsvorschriften, z.B.: a) spezialgesetzliche Regelung b) § 10 Abs. 1 DSG-LSA, wenn die Verarbeitung zur rechtmäßigen Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und keine besondere Rechtsvorschrift besteht c) § 4 Abs. 1 DSG-LSA (Einwilligung des Betroffenen)
5	Kreis der Betroffenen:	Bezeichnung des Personenkreises, dessen Daten erhoben, verarbeitet oder genutzt werden (z.B. Gewerbetreibende, Einwohner des Landkreises)
6	Art der Daten:	Auflisten der einzelnen Daten (z.B. Name, Vorname, Geburtsdatum ...)
7	vorgesehene Empfänger:	Vorgesehene Empfänger sind solche, an die nach vorab festgelegten Regeln unter bestimmten Voraussetzungen personenbezogene Daten weitergegeben oder übermittelt werden, auch durch Bereithalten zum Abruf. Einzutragen ist in Spalte 5./6. die genaue Bezeichnung der Empfänger. Dies können sein: a) andere Organisationseinheiten innerhalb der verantwortlichen (speichernden) Stelle, b) Dritte, an die Daten übermittelt werden (werden personenbezogene Daten ins Internet eingestellt, liegt darin wegen der Möglichkeit des weltweiten Abrufs stets auch eine vorgesehene/geplante Übermittlung in Drittstaaten), c) Stellen, die personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

8 Der Zweck der Weitergabe oder Übermittlung ist kurz darzustellen.

9 Die Ausführungen zu 4 gelten entsprechend.

10 Drittländer sind Länder außerhalb der EG oder anderer Vertragsstaaten des Abkommens über den europäischen Wirtschaftsraum (das sind Island, Norwegen und Lichtenstein).

11 Die Unterspalte A ist nur anzukreuzen, wenn die einzelnen Daten durch automatisierte Abrufverfahren zur Übermittlung bereitgehalten werden.

12	Regelfristen für die Löschung oder die Prüfung der Erforderlichkeit weiterer Speicherung:	diese können sich ergeben aus speziellen Regelungen, z.B. Gesetz oder Verwaltungsvorschrift z.B. a)... Jahre nach der Erstellung/letzten Änderung b) § 16 Abs. 2 Satz 1 Nr. 2 DSG-LSA
13	Zugriffsberechtigte:	gemeint sind nur Zugriffsberechtigte innerhalb der verantwortlichen Stelle

14 Es sind die von der verantwortlichen Stelle getroffenen technischen und organisatorischen Maßnahmen schriftlich festzulegen und entsprechend in einer Anlage zu erläutern (Beispiele für Maßnahmen vgl. Nrn. 6.2.1 bis 6.2.6 VV-DSG-LSA)

15	Art der Geräte (Hardware):	Auflisten der eingesetzten Informations- und Kommunikationstechnik (IuK) u.a. nach Typ, Anzahl und Standorten einschließlich Angaben zur Netzwerktopologie (LAN), die in der öffentlichen Stelle zum Einsatz kommt (gegebenenfalls zusätzliche Anlagen und Übersichten beifügen)
16	Art der Geräte (Hardware) zum Anschluss an Fremdnetze:	Die Ausführungen zu 15 gelten entsprechend. Auflisten der IuK, die speziell zum Anschluss an Fremdnetze benötigt wird und zum Einsatz kommt, wie z.B. Firewall- und Router-Technik, Switches, Hubs u.ä.
17	eingesetzte Software:	Auflisten der eingesetzten Software für den Betrieb der IuK. (Betriebssysteme, Anwendungssoftware, Datenbankbetriebssysteme u.ä.), die in der öffentlichen Stelle zum Einsatz kommt (gegebenenfalls zusätzliche Anlagen und Übersichten beifügen)
18	eingesetzte Software zum	Die Ausführungen zu 17 gelten entsprechend. Auflisten der eingesetzten Software für den Betrieb der IuK, die speziell zum Anschluss an Fremdnetze zum Einsatz kommt.

Anlage 5 zur Dienstanweisung Datenschutz und Datensicherheit

Prüfansätze zur Verfahrensfreigabe

1. datenschutzrechtliche Freigabe	ja	nein	prüfen
- wurde das Verfahren datenschutzrechtlich geprüft und bewertet? - existiert eine aussagefähige Beschreibung der Datenstruktur für alle im Verfahren genutzten und verarbeiteten Daten? - wurde geprüft, ob die Speicherung, Verarbeitung und Übermittlung der einzelnen Datenarten zulässig ist? - enthält die Datenstruktur Freitextfelder, die vorreserviert werden und denen erst später eine bestimmte Bedeutung zukommen soll? Wenn ja, . wurde die Zulässigkeit geprüft und . wurden für diese Freitextfelder bestimmte Auflagen festgelegt? - existieren bedarfsgerechte Zugriffsberechtigungen? - sind die Benutzerrechte aussagefähig dokumentiert? - ist eine Protokollierung für den Zugiff der Datenbasis vorgesehen, und zwar . beim Lesen oder . bei der Veränderung? - ist ein automatisiertes Abrufverfahren vorgesehen? - enthält das Verfahren ein angemessenes Sicherheitskonzept? - ist festgelegt, wer für das System verantwortlich ist? - werden alle Verfahrensänderungen maschinell protokolliert? - ist die Benutzerverwaltung (Einrichten, Rechtevergabe, Löschen) ausreichend dokumentiert? - existiert für das Verfahren ein eigener Benutzerservice? - ist dokumentiert . welche Personen der Benutzerservice (Angaben der Personen) einschließt? . auf welche Daten der Benutzerservice Zugriff hat? - werden die Zugriffe des Benutzerservice protokolliert?			

2. Fachliche Freigabe	ja	nein	Prüfen
a) Programmiertechnik - existieren verbindliche Programmierrichtlinien? - ist das Verfahren für die Änderung der Programme festgelegt? - wird bei allen wesentlichen Änderungen auf die Vollständigkeit der Dokumentation und die Revisionsfähigkeit geachtet?			

2. Fachliche Freigabe	**ja**	**nein**	**prüfen**
b) Programmtest - ist festgelegt . welche Daten für den Programmtest und welche für den Abschlusstest verwendet werden dürfen? . wer geeignete Testdaten zur Verfügung stellt? . welche Stelle für die Formulierung des Programmier- und Änderungs-auftrages zuständig ist? - wird beim Programmtest und für die Programmpflege Fremdpersonal eingesetzt? - wird bei der Programmpflege von der Fernwartung Gebrauch gemacht? c) Dokumentation - existiert eine Dokumentation darüber, welches Programm welche anderen Programme aufruft, welche Dateien verarbeitet und aus welchen Einzelkomponenten besteht? - enthält das Programmverzeichnis die Grunddaten: . Programmname mit Versionsnummer (evtl. Kurzbezeichnung) . Datum der Freigabe . Autor und Bearbeiter? - liegt eine aktuelle Programmbeschreibung (verbal oder graphisch) vor? - gibt es ein Bedienungshandbuch, das alle für die Benutzung des Programmes notwendigen Hinweise enthält und alle Eingabedaten ausreichend erklärt? - sind alle verfahrensspezifischen Nachrichten, die das Programm an den Benutzer richtet, dokumentiert? - sind alle verfahrensspezifischen Nachrichten und die möglichen Reaktionen von seiten des Benutzers in dem Benutzerhandbuch zusammengefasst? - liegt eine aktuelle Beschreibung aller zu verarbeitenden Dateien vor (Dateiname sowie Beschreibung des Datensatzes)? - ist die Testumgebung ausreichend dokumentiert? - wird diese Testumgebung auch bei Programmänderungen durchlaufen? - sind die verschiedenen Betriebsarten, unter denen das Verfahren ablaufen kann, ausreichend beschrieben? - sind die Schnittstellen zu anderen Programmsystemen ausreichend dokumentiert?			

2. Fachliche Freigabe	**ja**	**nein**	**prüfen**
d) Programmfreigabe Eine Kurzbeschreibung des Verfahrens ist der Freigabebescheinigung als Anlage beigefügt. Es handelt sich um: - Einführung eines neuen DV-Verfahrens/Programms - Änderung eines bestehenden DV-Verfahrens/Programms Art der Änderung, Beschreibung als Anlage - ist sichergestellt, dass alle Anwender ausreichend in das neue Programm eingewiesen sind?			

Anlage 6 zur Diensanweisung Datenschutz und Datensicherheit

Einsatz und Betrieb der Informations- und Kommunikationstechnik für das Haushalts- und Kassenwesen der Kreisverwaltung Mansfeld-Südharz

1. **Allgemeines**

Für die Buchführung gilt diese Dienstanweisung in Verbindung mit der Dienstanweisung für die Kreiskasse vom 18.07.2007

2. **Richtige Verarbeitung**

2.1 Datenermittlung ist das Erstellen besonderer Erfassungsbelege und die erfassungsgerechte Aufarbeitung vorhandener Belege (Urbelege).

Die datenermittelnde Stelle bescheinigt im Anordnungswesen auf den Belegen, dass die Daten vollständig und richtig ermittelt werden.

Sie ist für die ordnungsgemäße und vollständige Übergabe der Erfassungsbelege bzw. selbst gefertigten Anordnungsbelege an die Kreiskasse verantwortlich.

Grundlagen für die Datenermittlung sind insbesondere:
a) Zahlungs- und Buchungsanordnungen
b) Gutschriften der Kreditinstitute
c) einzureichende Schecks
d) Einzahlungsquittungen
e) Auszahlungsquittungen
f) Durchschriften von Aufrechnungsmitteilungen
g) Lastschriften der Kreditinstitute

Die Kreiskasse ist für die bei der Abwicklung der Kassengeschäfte anfallenden Daten zuständig und für die richtige, vollständige und rechtzeitige Aufarbeitung verantwortlich. Dazu gehören:
a) Eingangs- und Ausgangsrechnungen durch die von der Kämmerei bestimmten Fachämter
b) Buchung der Einzahlungen und Auszahlungen (bar, unbar, Verrechnung)
c) Aussetzung der Vollziehung und Setzen der Mahnsperren
d) Übernahme der Bankabbucher
e) Sollstellung von Nebenforderungen.

Für die Datenübermittlung sind die vom Programm erstellten Belege zu verwenden. Mögliche Abweichungen regelt die Amtsleiterin der Kämmerei in einer schriftlichen Anweisung.

Die Ziffern, Buchstaben und zugelassenen Sonderzeichen sind stellengerecht in die einzelnen Felder der vorgegebenen Datenmaske einzutragen.

Der Kassenverwalter bestimmt die Unterschruftsleistung auf dem Bankkonto.
Die Vorschriften der Dienstanweisung für das Anordnungswesen vom 26.07.2007 bleiben unberührt.

Die Kreiskasse kontrolliert die Datenbelege nach § 6 GemKVO.

Vor dem Druck der Anordnungsbelege sind die Anordnungen auf Vollständigkeit und Richtigkeit zu prüfen.
Danach sind durch die Fachämter die Anordnungen zu fertigen.
Der Kreiskasse sind die Anordnungsbelege zu übergeben.

2.2 Datenerfassung
Die von der Kämmerei mit der Datenerfassung beauftragten Stellen sind auch für die erfassten Ergebnisse nach der Richtigkeit und Vollständigkeit verantwortlich.
Eigene Kontrollen der erfassten Daten sind obligatorisch. Dabei erkannte Erfassungsfehler sind sofort zu berichtigen.

2.3 Datenverarbeitung
Die Daten der anordnenden Dienststellen und der Kreiskasse werden durch Client-PC im Rahmen einer Client-Server-Lösung der Firma AB-DATA verarbeitet. Die Datenhaltung erfolgt auf dem Server des Bereiches der EDV.

3. **Datensicherung**
Die Daten des HKR-Programmes sind mindestens einmal täglich, alle anderen Anwendungen mindestens einmal wöchentlich zu sichern.

Anlage 7 zur Dienstanweisung Datenschutz und Datensicherheit

Regelungen für den Einsatz von E-Mail

Die elektronische Post - E-Mail - wird zunehmend als Kommunikationsmittel eingesetzt und ersetzt in vielen Fällen Briefpost und Faxversand.

Der papiergebundene Schriftverkehr kann jedoch nicht in allen Fällen durch elektronische Datenübertragung ersetzt werden. Nur soweit zulässig, technisch möglich und sicher genug soll dem elektronischen Datenaustausch der Vorrang eingeräumt werden.

Für den Bereich der elektronischen Post sind Regelungen erforderlich, um die Sicherheit hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit der elektronisch übertragenen Informationen zu gewährleisten.

Wegen noch fehlender bzw. nicht eingesetzter Verschlüsselungsmechanismen und digitaler Signaturen kann die E-Mail nur mit Einschränkung verwendet werden.

1. Allgemeine Grundsätze

1.1 Die nachstehenden Regelungen sind anzuwenden auf externe und interne elektronische Post, deren Behandlung, Übermittlung und Eingangsbearbeitung.
Soweit in dieser Anlage keine besonderen Festlegungen getroffen werden, gelten die sonst einschlägigen Vorschriften und Dienstanweisungen des Landkreises Mansfeld-Südharz.

1.2 Das E-Mail-System dient dem **dienstlichen Nachrichtenaustausch** des Nutzers und darf daher nur für dienstliche Belange verwendet werden. Eine Nutzung zu privaten Zwecken ist nicht zulässig. Sämtlicher ein- und ausgehenden E-Mails werden datenschutz- und und dienstrechtlich wie Briefpost behandelt. Gehen private E-Mails ein, werden diese wie private schriftliche Post behandelt. Sie werden den betreffenden MitarbeiterInnen zugeleitet, sind von diesen dann aber unverzüglich zu löschen.

1.3 Grundsätzlich beschränkt sich der Nachrichtenaustausch per **externer E-Mails** auf Schriftstücke und Nachrichten ohne vertrauliche oder geschützte Informationen und ohne personenbezogene Daten.
Bei externen Versand von Nachrichten muss sich jeder Nutzer bewusst sein, dass öffentliche Netze zur Übertragung genutzt werden. Hierbei werden die Nachrichten über verschiedene in der Regel unbekannte Systeme weitergeleitet und auch temporär zwischengespeichert. Dies ist ein erhebliches Gefahrenpotential. (Grundsatz: E-Mail ist mit einer Postkarte zu vergleichen).
Deshalb ist der Versand von Informationen, die einem besonderen Schutz unterliegen, grundsätzlich nicht zulässig.
Generell ist es untersagt, datenschutzrelevante Daten, personenbezogene Daten, Personal- und Sozialdaten und anderweitig vertrauliche Daten per E-Mail extern zu übertragen. Dies gilt nicht nur für den Inhalt der E-Mail, sondern auch für beigefügte Anlagen.
Ausnahmen sind mit Zustimmung des Fachbereiches 1, Sachgebiet EDV möglich, wenn z.B. ein freigegebenes kryptografisches Sicherungsverfahren (Verschlüsselungsprogramm) eingesetzt wird.

Es ist außerdem darauf zu achten, dass aus Gründen der Rechtssicherheit keine rechtserheblichen oder termingebundenen Mitteilungen per E-Mail übermittelt werden.

Der Abschluss von rechtsverbindlichen Geschäften über externe E-Mails ist nicht zulässig.

1.4 Daten des Mailverkehrs werden systematisch protokolliert. Diese Logdateien werden vom Fachbereich 1, Sachgebiet EDV nur für Zwecke des Daten- und Systemschutzes, der Systemkonfiguration sowie für die Sicherstellung des ordnungsgemäßen Betriebes oder Abrechnungszwecke verwendet. Innerhalb des Sachgebietes EDV bleiben die Zugriffe auf diese Daten auf die mit der technischen Administration des Systems betrauten Personen beschränkt.
Der Landrat hat grundsätzlich das Recht, die Einhaltung der Regelungen, insbesondere die ausschließlich dienstliche Nutzung von E-Mails, stichprobenartig zu überprüfen.
Von einer solchen Kontrolle ausgenommen sind die Personalvertretung, die Schwerbehindertenvertretung und die Gleichstellungs-/Behinderten- und Ausländer-beauftragte. Ebenso ausgenommen von einer stichprobenartigen Kontrolle sind die MitarbeiterInnen, denen in ihrer dienstlichen Tätigkeit persönliche Geheimnisse anvertraut werden, soweit durch eine Kenntnisnahme des Inhalts der Nachricht oder die Auswertung der Daten ein Rückschluss auf die betroffene Person möglich ist.

Bei konkretem Missbrauchsverdacht kann eine gezielte Überprüfung im Einzelfall erfolgen. Dazu wird die Zustimmung des Personalrates eingeholt. Bei der Überprüfung selbst ist der Datenschutzbeauftragte hinzuzuziehen.

Maßnahmen, die den Missbrauch der E-Mail-Nutzung verhindern oder beweisen helfen, können, wenn ein begründeter Verdacht vorliegt, bei Gefahr im Verzug unmittelbar angeordnet und durchgeführt werden. In diesen Fällen sind der Personalrat und der Datenschutzbeauftragte anschließend unverzüglich zu unterrichten.

Alle genannten Kontrollen werden vom Landrat angeordnet und von den dafür verantwortlichen Administratoren im Sachgebiet EDV durchgeführt.
Über das Ergebnis berichtet der Landrat den Personalrat.
Eine Auswertung des Systems durch die Dienststelle für Zwecke der Verhaltens- und Leistungskontrolle findet nicht statt.

2. **Organisatorische Grundsätze**

2.1 Auf Antrag der Organisationseinheit setzt das Sachgebiet EDV die organisatorischen Maßnahmen für die Teilnahme am E-Mail-Betrieb um.

2.2 Die im System eingerichteten MitarbeiterInnen erhalten eine eigene E-Mail-Adresse.

2.3 Es ist eine zentrale E-Mail-Adresse für den Landkreis eingerichtet.
Sie lautet: landkreis@mansfeldsuedharz.de
Bearbeitet wird dieses E-Mail-Konto von der Pressestelle der Kreisverwaltung Mansfeld-Südharz.

2.4. Die bestehenden Regelungen über die Behandlung von Postein- und -ausgängen sind grundsätzlich auch auf E-Mails anzuwenden.
Elektronisch eingehende Post von "Aufsichtsbehörden" ist unverzüglich dem Dienst-vorgesetzten zuzuleiten.

2.5. Aus datenschutzrechtlichen Gründen ist darauf zu achten, dass Informationen nur diejenigen MitarbeiterInnen erhalten, die die Information erhalten dürfen.

2.6 Elektronisch erstellte Dokumente sind, soweit sie für den Geschäftsgang von Bedeutung sind, in Papierform zu den Akten zu nehmen. Die E-Mails werden zwar gesichert, das System ist aber nicht als elektronische Archivierung verwendbar.

2.7 Nicht mehr benötigte E-Mails sollen möglichst zeitnah vom Anwender in eigener Verantwortung gelöscht werden.

2.8 Alle eingehenden und ausgehenden Mails incl. der Anhänge werden zentral auf einem gesonderten Server auf Virenbefall kontrolliert. Wird ein Virenbefall festgestellt sind die verantwortlichen Administratoren im Sachgebiet EDV befugt, zum Schutz des IT-Systems diese ggf. zu löschen. Dies gilt auch für privat eingehende E-Mails.

Ein absoluter Schutz ist auf diesem Wege jedoch nicht erreichbar. Einmal eingeschleppte Viren können sich rasch in dem gesamten System verbreiten. Um dieses Restrisiko weiter einzuschränken, sollten **grundsätzlich keine Eingänge von unbekannten Absendern von E-Mails geöffnet oder gestartet werden, die einen dienstlichen Bezug nicht erkennen lassen.**
Unseriös oder zweifelhaft erscheinende E-Mails sind daher nicht zu öffnen. Die BenutzerInnen sind verpflichtet, sicherheitsrelevante Beobachtungen und Ereignisse unverzüglich dem Sachgebiet EDV zu melden. Das Sachgebiet EDV wird dann eine kurzfristige Überprüfung vornehmen.

3. Empfang elektronisch übermittelter Dokumente

3.1 Das Mail-Postfach ist von der/dem Mitarbeiter/in mehrmals täglich auf den Eingang elektonischer Post zu kontrollieren.
Jede/r Mitarbeiter/in ist für die ordnungsgemäße Behandlung elektronischer Posteingänge verantwortlich.

Fehladressierte E-Mails sind, soweit der tatsächliche Empfänger ersichtlich ist, unmittelbar an den tatsächlichen Empfänger weiterzuleiten. Anderenfalls ist die E-Mail zur Zuständigkeitsermittlung an die zentrale Mailstelle zuzustellen oder mit einem entsprechenden Hinweis an den Absender zurückzugeben.

3.2 Auch wenn E-Mails formal nicht die an die Schriftform gebundene Willenserklärung geltenden Voraussetzungen erfüllen, sind sie jedoch als Willenserklärung anzusehen und entsprechend zu behandeln. Zur Rechtssicherheit sollte eine eingegangene Willens-erklärung noch mal in Schriftform angefordert werden.

3.3 Beim Eingang rechtserheblicher Erklärungen (z.B. Widerspruch) per E-Mail (ohne qualifizierte digitale Signatur) sind die zuständigen Stellen verpflichtet, den Absender unter Bezug auf die E-Mail, in schriftlicher Form auf den Formmangel hinzuweisen.

3.4 Können Dokumente nicht mit den am Arbeitsplatz zur Verfügung stehenden Hilfsmitteln geöffnet und gelesen werden, so ist das Sachgebiet EDV umgehend zu